Dell OpenManage Power Center Version 1.0 User Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this document is subject to change without notice.
© 2012 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL™ logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core™ and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD®, the AMD logo®, and combinations thereof, are registered trademarks and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE ™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter®, and vSphere® are registered trademarks or trademarks of VMWare, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

February 2012

Contents

1 Overview 11

Features **11**

Topology **12**

System Requirements **13**

Hardware Requirements for Server System 13

Software Requirements for Server System 13

Hardware and Software Requirements for Devices 14

Supported Devices 14

2 Getting Started 16

Management Console Introduction **16**

Use Case Introduction **18**

Use Case 1: Installing Power Center **19**

Use Case 2: Logging into Power Center **19**

Use Case 3: Adding a Device from the Network **19**

Use Case 4: Managing Devices **20**

Use Case 5: Creating the Data Center Group Structure **20**

Use Case 6: Monitoring Power / Temperature / Events of a Device or Group **21**

Use Case 7: Creating Power Policies **21**

Use Case 8: Comparing Two or More Devices/Groups . . . **21**

3 Installing and Launching 23

Installing Power Center **23**

Installed Directories **26**

Power Center Services **26**

Uninstalling Power Center **27**

Launching Power Center **28**

Configuring ESC for Internet Explorer **28**

4 Access Control 30

About Authentication **30**

Logging in **30**

About Login 30

Log in with User Name and Password 31

Log in with Single Sign-on (SSO) 35

Multiple User Login 39

Logging out **40**

Managing User Roles **40**

Adding a Role 40

Updating a Role 41

Deleting a Role 41

Managing User Accounts **41**

Adding a User 41

Updating a User 42

Deleting a User 42

Managing Privileges 43

Global Configuration 46
Device Discovery 47
Manage Role/User 47
View Device/Group 47
Manage Device/Group 47
Manage Policy 48
Manage Event 48
Manage License 49

Viewing Current User Information 49

Licensing 49

Importing License 49
Viewing License 50

5 Device Discovery 51

Supported Devices and Unsupported Devices 51

Adding a Device from the Network 52

Adding a Device Manually 54

Rediscovering Devices in a Chassis 55

Protocol Profile 56

6 Device Management 58

Viewing Devices 58

Editing Devices 60

Editing Protocol **61**

Deleting Devices **61**

Filtering Devices **62**

Sorting Devices **63**

7 Group Management 64

Mapping Group Structure Information **64**

Finding a Group or Device **65**

8 Physical Groups 67

Data Center Physical Group **67**

Creating Physical Group **67**

Managing Physical Groups **68**

Adding Devices to a Physical Group 68

Editing Devices in a Physical Group 70

Removing Devices from a Physical Group 70

Moving Devices in a Physical Group 71

Moving a Physical Group 71

Editing Physical Groups **72**

Deleting Physical Groups **72**

Viewing Physical Groups **72**

9 Logical Groups 74

Creating a Logical Group **74**

Managing Logical Groups 74
Adding a Logical Group 74
Adding Devices or Groups to a Logical Group . . 75
Editing Logical Groups 76
Deleting Logical Groups 76
Viewing Logical Groups 76

10 Power Monitoring 78

Power Monitoring Level 78
Power Monitoring Configuration 78
Viewing Power Details 80
Viewing Energy Consumption 82
Monitoring PDU Power 83
Monitoring UPS Power 84
Power Dashboard 85
Printing Power Monitoring/Dashboard Graph 87

11 Temperature Monitoring 88

Temperature Monitoring Level 88
Temperature Monitoring Configuration 88
Viewing Temperature Details 89
Monitoring Temperature of Chassis/Blade Server . . . 92

Monitoring Temperature of Devices/Groups 92

Temperature Dashboard 92

Printing Temperature Monitoring/Dashboard Graph . . 94

12 Power Policies 95

How Does a Dynamic Power Policy Work? 96

Power Policy Capabilities 97

Upgrading Device Power Policy Capability 98

Creating a Policy 98

Viewing Policy Details 101

Policy Priority Levels 101

Policy Modes 102

Enabling/Disabling Policy 102

Displaying Policies in the Power Details Graph 103

Updating a Policy 103

Deleting Policies 103

Filtering Policies 104

Emergency Power Reduction 104

Policy-Related Events 105

13 Comparing 106

Changing the Time Period 106

Adding a Device or Group 107

Removing/Changing Device or Group 107

Printing the Comparison Result 108

14 Event Management 109

Pre-defined Events 109

Custom Events 112

Supported PDU/UPS Events 114

Event Severity Levels 115

Viewing Events 115

Sorting Events 116

Editing Events 116

Deleting Events 116

Filtering Events 117

Filtering Events by Group/Device 118

Sending Test Events from an IPMI Device 118

15 Security 120

Starting Services with a Normal Windows OS User Account 120

OS Hardening 122

Audit Log 123

Managing Certificates 124

16 Configuring Power Center 126

Monitoring Settings **126**

Default Units Settings **127**

Protocol Type Device Timeout Settings **128**

Energy Consumption Settings **128**

SNMP Traps Settings **128**

Database Policy Settings **130**

Installation Settings **132**

Database Settings 132

Kerberos Realm Settings 138

Power Center Server's Domain Account for Kerberos SSO 138

17 Backup and Recovery 139

Power Center Data **139**

Power Center Backup **140**

Power Center Recovery **141**

18 Troubleshooting 144

1

Overview

Dell OpenManage Power Center is a power management solution for the data center. It enables you to monitor and manage power consumption and temperature in your data center through the management console.

Features

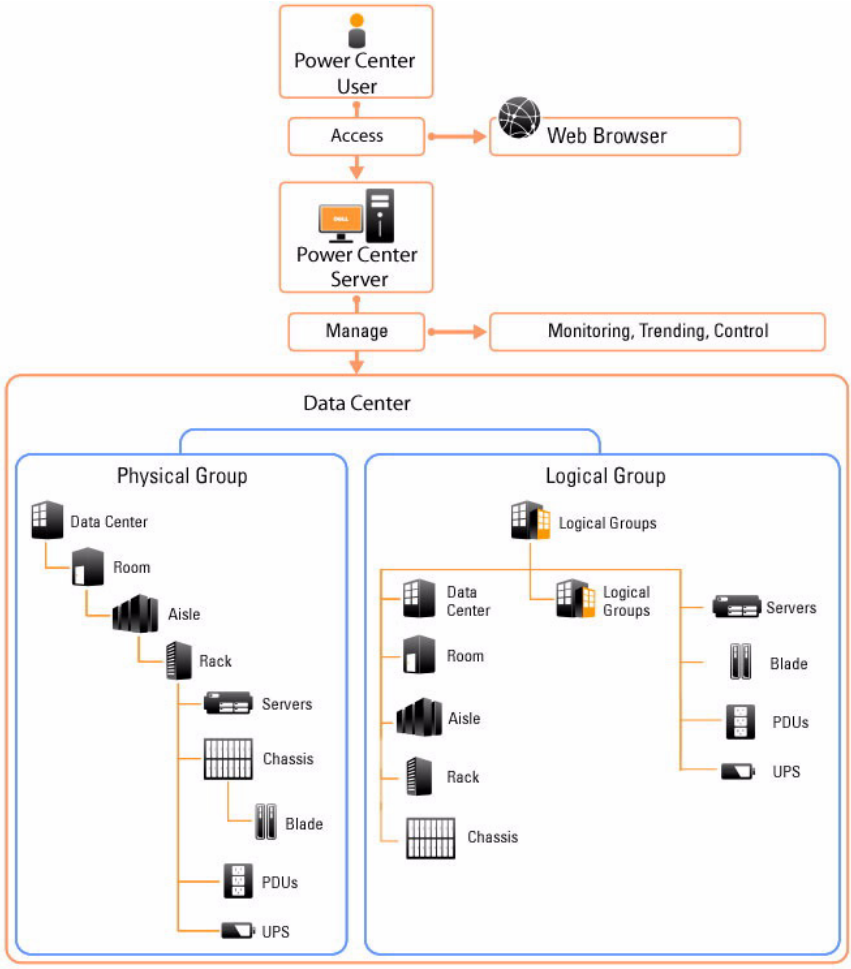
The following table lists the features provided by OpenManage Power Center.

Table 1-1. Product Features

Feature	Description
Power Monitoring	Monitors power related metrics on several levels: • Individual device • Data center/Room/Aisle/Rack/Chassis • User-defined group
Temperature Monitoring	Monitors data center temperature data.
Power Control	Creates policies that can control the data center power consumption at the device and group level.
Device Discovery	Supports Dell enterprise systems including PowerEdge blade and tower/rack servers, chassis, and many different PDUs and UPS.
Role-based Access Control	Supports user authentication and multiple role-based privilege levels.
Event Management	Monitor and manage device/group events.

Topology

The following figure shows how to use a Web browser to access the Power Center server and manage the data center.



System Requirements

Hardware Requirements for Server System

You must install Power Center on a system with at least:

- A dual-core processor of 2.6Ghz or higher
- 4GB RAM
- 60GB free space of hard drive
- Gigabit bandwidth of network infrastructure

Software Requirements for Server System

Power Center supports the following operating systems:

- Microsoft Windows 2003 Standard/Enterprise/Small Business Server SP2 (x86, x64)
- Microsoft Windows 2003 Standard/Enterprise/Small Business Server R2 (x86, x64)
- Microsoft Windows 2008 Standard/Enterprise/Datacenter (x86, x64)
- Microsoft Windows 2008 R2
- Microsoft Windows 7
- Microsoft Windows Vista (x86, x64)

Power Center supports the following Web browsers:

- Mozilla Firefox 5.0 and 6.0
- Microsoft Internet Explorer 7.0, 8.0 and 9.0

Power Center is validated to work with the following virtualization environment:

- VMware ESX (3.5/4.0)
- Microsoft Server 2008 Hyper-V

The Power Center installation includes the following major software tools:

- Sun Microsystems Java Runtime Environment (JRE) 6
- Apache Tomcat application server
- PostgreSQL 8.3.5

Hardware and Software Requirements for Devices

Power Center defines the following hardware and software requirements for supported devices:

- The server device must comply with Dell iDRAC6/iDRAC7.
- Power Distribution Unit (PDU) or Uninterruptable Power Supply (UPS) devices comply with the Management Information Base (MIB) provided by their vendor through SNMP interface.
- The device must provide exclusive access for Power Center. This is because the policies set on the devices from other management software will impact the Power Center power control function.
- The Baseboard Management Controller (BMC) user, through which Power Center communicates with devices, must be a local user with Administrator role. The device must be configured to allow the Administrator to use at least one of the cipher suite levels 0-3, and enable the "IPMI over LAN" setting.
- The WS-MAN user, through which Power Center communicates with the chassis, must be a local user with Administrator role. The chassis must be configured to enable the "Web Server" service.

Supported Devices

Power Center supports up to 2000 managed devices in one data center.

The following devices are validated and supported by Power Center:

Table 1-2. Supported Devices

Category	Supported Platform	Validated Model
Server	Dell	• Dell PowerEdge R610 Rack Server • Dell PowerEdge R620 Rack Server • Dell PowerEdge R710 Rack Server • Dell PowerEdge R720 Rack Server • Dell PowerEdge M610 Blade Server • Dell PowerEdge M620 Blade Server • Dell PowerEdge T620 Tower Server
Chassis	Dell	• Dell PowerEdge M1000e Blade Enclosure

Table 1-2. Supported Devices

Category	Supported Platform	Validated Model
PDU	Dell	• Dell 6804 Metered PDU • Dell 6607 Metered PDU • Dell XX5T6 Metered PDU • Dell 6803 Metered PDU • Dell 6605 PDU
	APC	• APC Metered Rack PDU AP78001 • APC Switched Rack PDU AP7900 • APC Switched Rack PDU AP7920
	Eaton	• Eaton Monitored PDU PW312MI0UC07 • Eaton Switched PDU PW105SW0U154
	Emerson	• Emerson Liebert MPH MPH-NCR09NXXE30
	ServerTech	• ServerTech Switched PDU CW-24V4J411 • ServerTech Smart CDU, 0U CS-24V1-C20M
UPS	Dell	• Dell N313P Line interactive UPS w/ web card H910P • Dell Online Rack UPS 3750R OL K804N • Dell UPS, 2700/2300VA, 120V, 3U K802N
	APC	• APC Online UPS w/ Web card SURTD3000XLI • APC Smart-UPS 3000VA RM SUA3000RM2U • Smart-UPS 5000VA RM DL5000RMT5U
	Eaton	• Eaton Line interactive UPS w/ Web card PW5130I1750-XL2U
	Emerson	• Emerson Online UPS w/ Web card GXT2-2700RT208

2

Getting Started

This chapter introduces the Power Center management console and presents several use cases that describe standard usages of Power Center.

Management Console Introduction

To use the Power Center functions, you must open a Web browser and log into Power Center.

After you log into Power Center, the management console opens with a list of the available pages in the left navigation pane, and the currently-open page appearing in the right pane.

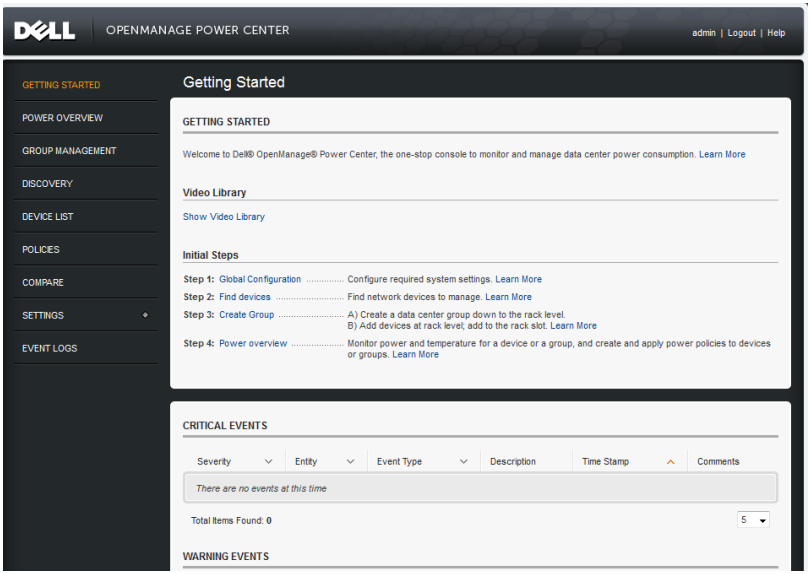

DELL
OPENMANAGE POWER CENTER
admin | Logout | Help
GETTING STARTED
POWER OVERVIEW
GROUP MANAGEMENT
DISCOVERY
DEVICE LIST
POLICIES
COMPARE
SETTINGS
EVENT LOGS
Getting Started
GETTING STARTED
Welcome to Dell® OpenManage® Power Center, the one-stop console to monitor and manage data center power consumption. Learn More
Video Library
Show Video Library
Initial Steps
Step 1: Global Configuration ..... Configure required system settings. Learn More
Step 2: Find devices ..... Find network devices to manage. Learn More
Step 3: Create Group ..... A) Create a data center group down to the rack level.
B) Add devices at rack level; add to the rack slot. Learn More
Step 4: Power overview ..... Monitor power and temperature for a device or a group, and create and apply power policies to devices or groups. Learn More
CRITICAL EVENTS
Severity
Entity
Event Type
Description
Time Stamp
Comments
There are no events at this time
Total Items Found: 0
5
WARNING EVENTS

Table 2-1. Available Actions

Main Page	Available Actions on This Page
Getting Started	This page introduces the Dell OpenManage Power Center features and the initial setup steps, and lists additional tasks you can complete after the setup. You can select a video from the video liberary to help you get started, or you can click help links to get additional information.
Power Overview	This page enables you to view or edit data center power information of a physical group or logical group, and view the information of devices in a rack or chassis. This page includes these tabs: Events, Dashboards, Power Details, Temperature Details, Policies, Thresholds.
Group Management	This page enables you to set up and organize your devices into physical or logical groups.
Discovery	This page discovers supported devices in the data center network. After a device is discovered, it is automatically added to the Device List page, and can be managed by Power Center. From this page, you can: • View the active searches • View the recent discovery jobs • Rerun a search using the discovery search criteria
Device List	This page lists network-discovered devices and devices added manually. From this page, you can: • Add supported or unsupported devices to the Device List page • Remove devices from the Device List page • Edit device information for a single device or multiple devices • Edit protocol information for a single device • Filter and sort devices to meet current needs
Policies	This page enables you to manage the power policies.

Table 2-1. Available Actions

Main Page	Available Actions on This Page
Compare	This page enables you to compare power and temperature status and energy consumption between the selected groups/devices. You can also print the comparison results.
Settings → Settings	This page enables you to view or configure all the settings.
Settings → User Accounts	This page enables you to set up and manage the user accounts.
Settings → Licensing	This page enables you to view or import the license.
Event Logs	This page lists all events at all severity levels. From this page, you can: • View all events • Add comments to events • Delete the events • Filter and sort the events

Use Case Introduction

This section provides several standard usage scenarios to help you get started with Power Center, or refresh your knowledge of Power Center functionality.

If you are a first-time user, you can follow the sequence of use cases 1- 5 to install and set up the group structure for Power Center monitoring of your data center. After you set up your data center for monitoring, you can refer to use case 6, 7 or 8 to use Power Center for monitoring, comparing power and temperature data between devices and/or time slots, and creating policies.

If you are an experienced user, you can refer to any use case for a quick reference on how to complete tasks.

1. Installing Power Center
2. Logging into Power Center
3. Adding a device from the network
4. Managing devices

5 Creating the data center group structure
6 Monitoring power/temperature/events of a device or group
7 Creating power policies
8 Comparing two or more devices/groups

Use Case 1: Installing Power Center

This use case describes how to install Power Center.

1 Make sure the system meets the software and hardware requirements.

   See "System Requirements" in the "Overview" chapter.

2 Click OpenManagePowerCenter.exe to start installation.

   See "Installing Power Center" in the "Installing and Launching" chapter.

Use Case 2: Logging into Power Center

This use case describes how to launch and log into Power Center.

1 Open your Web browser.
2 You may need to configure your Web browser to launch the Power Center management console.

   See "Configuring ESC for Internet Explorer" in the "Installing and Launching" chapter.

3 Enter the Power Center management console address: **https://**<*Server_Name*>:<*HTTPS_Port*>**/powercenter/**

   See "Launching Power Center" in the "Installing and Launching" chapter.

4 Select a user account and enter your user name and password.

   See "Logging in" in the "Access Control" chapter.

5 The Power Center management console appears. You can start to use Power Center functions.

Use Case 3: Adding a Device from the Network

This use case describes how to discover devices from the network of your data center.

1 Go to the **Discovery** page to add devices from the network.

2 Configure the search criteria for the devices you want to discover.

See "Adding a Device from the Network" in the "Device Discovery" chapter.

3 The discovered devices appear in the **Device List** page.

Use Case 4: Managing Devices

This use case describes how to manage devices after they are discovered.

1 Go to the **Device List** page, select the devices you want to manage, then delete/edit/filter them.

2 Or you can click **Add** in the **Device List** page to add a device manually then manage it.

See "Adding a Device Manually" in the "Device Discovery" chapter.

Use Case 5: Creating the Data Center Group Structure

This use case describes how to create the data center group structure.

1 Go to the **Group Management** page, click **Select a Physical Group**. Create the physical groups following this order: **Data Center** → **Room** → **Aisle** → **Rack** → **Chassis**.

See "Data Center Physical Group" in the "Physical Groups" chapter.

2 Add devices to the physical groups:

- A rack server can only be added to a rack.
- A blade server can only be discovered in a chassis.
- PDU, UPS and unsupported devices can be attached at any level of the physical group structure.

See "Adding Devices to a Physical Group" in the "Physical Groups" chapter.

Use Case 6: Monitoring Power / Temperature / Events of a Device or Group

This use case describes how to monitor power/temperature details and events of a device or group.

1. Go to the **Power Overview** page, and select the device or group you want to monitor.
2. Check the various tabs:
   - The **Power Details** tab shows the power details for the device/group.

     See the "Power Monitoring" chapter.
   - The **Temperature Details** tab shows the temperature details for the device/group.

     See the "Temperature Monitoring" chapter.
   - The **Events** tab shows the events for the device/group.

     See the "Event Management" chapter.

Use Case 7: Creating Power Policies

This use case describes how to create a power policy. Power policies allow you to cap power consumption and set priorities for the policies so that you can save power for your data center.

1. Go to the **Power Overview** page, and select a device or group.
2. Click **Policies** tab, and create a policy for this device/group.

   See "Creating a Policy" in the "Power Policies" chapter.
3. You can view policies for this device/group in this **Policies** tab. You can also go to the **Policies** page in the management console to view all policies in the data center.

Use Case 8: Comparing Two or More Devices/Groups

This use case describes how to compare the power/temperature status and the energy cost for two or three devices/groups.

1. Go to the **Compare** page.
2. Select two or three devices or groups to compare.

   See "Adding a Device or Group" in the "Comparing" chapter.
3. Set the time frame for comparison. You can use this feature to compare power/temperature data for the same devices/group in different time ranges.

   See "Changing the Time Period" in the "Comparing" chapter.
4. Optionally, click **Print** to print the comparison results. You may need to configure your Web browser before printing.

   See "Printing the Comparison Result" in the "Comparing" chapter.

3

Installing and Launching

This chapter explains how to install, uninstall and launch Power Center. After Power Center is installed, you may need to change the account for Power Center services for better security, or you can use a Web browser to launch the Power Center management console to start using it. You can also uninstall it when you no longer need it.

Installing Power Center

To install Power Center, you must have Administrator privilege. Otherwise, the installation may fail.

Before installing Power Center, verify that your system meets the minimum system requirements. See "System Requirements" in the "Overview" chapter.

Follow these steps to install Power Center:

1. Double-click the file **OpenManagePowerCenter.exe**.
2. In the installation wizard home page, click **Next**.
3. In the **License Agreement** screen, read the license agreement and select **I accept** ....Click **Next**.
4. In the **License** page, read the license message. Click **Next**.
5. In the **Destination Folder** screen, either leave the default installation path or browse to your desired installation path. Click **Next**.

NOTE: The installation path only supports ANSI characters (English characters, numbers, and simple symbols). Do not use an installation path with non-ANSI characters.

6. In the **OpenManage Power Center Setting** screen, configure the following HTTPS settings:
   - HTTPS Port — By default, Power Center uses port 8643 for HTTPS communication. To select a different port, enter the new port number. The port number must be a number between 2000 to 9000.
   - Keystore Password — Enter a keystore password. The password will be used to access the keystore file. After entering the password, in the **Verify Password** field, enter again to confirm.

NOTE: The password must be more than 5 characters, and cannot contain non-ANSI characters and double quotes (").

- HTTPS Certificate Information — Enter your information for the HTTPS certificate, including your name, organization, address, state, country code. The information will be used for certificate management.

Click **Next**.

7 In the **OpenManage Power Center Setting** screen, continue to enter the following information for the PostgreSQL database server account:

- Use another database server— This option enables you to install the Power Center database on a remote server. To use this option, the system must meet the following requirements:

– The remote server must have a running PostgreSQL database service (v8.3.5). You can download it from **http://www.postgresql.org**.

– There is no Power Center database on the remote server.

– The database service on the remote server is able to accept remote database connnection. For more information on this, see "Change to Database on a Remote System" in the "Configuring Power Center" chapter.

– The correct connection information (Server Name, Database Port, Database User Name, Database User Password) is provided.

If you enabled the option to use another database server, enter the following information about the database service on the remote server:

- User Name — Enter your PostgreSQL database server user name.
- User Password — Enter your PostgreSQL database server user password.

NOTE: The password must be a minimum of 8 characters in length with characters from at least three of the following categories: uppercase, lowercase, numeric, non-alphanumeric. It cannot include spaces.

- Verify password — Enter the password again to confirm.
- PostgreSQL Port — Default value is 6443. If another database is already using the default port, enter a different port.

- PostgreSQL Data Directory — The location of PostgreSQL data. If you enabled the option "Use another database server", you do not need to enter information for this field.

Click **Next**.

8 In the **OpenManage Power Center Setting** screen, continue to configure the Power Center super user account (also called installation account in the **User Accounts** page) settings, this account is used for logging into the Power Center management console:

- User Name — Enter a name for the super user, or leave the default name: admin.
- User Name rules —

a Must be unique for each Power Center user.

b Can be up to 20 uppercase or lowercase printable characters except " / \ [ ] : ; | = , + * ? < > . @.

c Case insensitive.

- User Password — Create the user password for the super user account.

NOTE: The password must be a minimum of 8 characters in length with characters from at least three of the following categories: uppercase, lowercase, numeric, non-alphanumeric, and can include spaces.

- Verify password — Enter the password again to confirm.

Click **Next**.

9 In the **Power Center Setting** screen, continue to configure the Kerberos settings. These options are optional, you can enable the option and configure the following settings to support SSO. For more information on SSO, see "Single Sign-on" in the "Access Control" chapter, or you can click **Next** to skip this step.

- Realm Name — Enter the Realm name (domain name) of KDC server.
- KDC Server — Enter the address of KDC server, it can be either an IP address or a server name.
- Kerberos Pre-authentication User Name — Enter the user name for the Kerberos pre-authentication account.

NOTE: User names with Chinese characters are not supported due to the limitation of Java Kerberos related library implementation.

- Kerberos Pre-authentication User Password — Enter the password for the Kerberos pre-authentication account.

Click **Next**.

10 In the **Ready to Install the Program** screen, click **Install**.

11 After installation completes, click **Finish** to exit the installation wizard.

Installed Directories

By default, the Power Center package installs to: **C:\Program Files\Dell\OpenManagePowerCenter**.

NOTE: You cannot install Power Center to the root folders of Windows volume. You must select a none-root folder or another volume to install.

The Power Center package includes the following folders:

Table 3-1. Installed Directories

Directory	Description
bin	Power Center binaries
conf	Power Center configuration files
external	Other applications installed by Power Center
Logs	Power Center event logs
Pgdata (default)	Database files

To protect your data, the following files are accessible only to Network Service or Administrator users:

- OpenManagePowerCenter\conf\app.config.xml
- OpenManagePowerCenter\external\apache-tomcat\conf\server.xml

Power Center Services

Power Center includes the following services:

- Dell OpenManage Power Center — Apache Tomcat server accommodating the Power Center web application which passes action requests to the Power Center server.
- Dell OpenManage Power Center Database Server — The PostgreSQL internal database for Power Center.
- Dell OpenManage Power Center SNMP Dispatcher — If Windows SNMP Trap service is installed, it reroutes SNMP traps to Dell OpenManage Power Center Server service. If Windows SNMP Trap service is not installed, this service will automatically stop.

  NOTE: If Windows SNMP Trap service is installed, make sure it is not disabled, otherwise Power Center cannot function properly.
- Dell OpenManage Power Center Server — The Power Center server core service. It carries out all actions, including communication with devices.

To stop or start a service, select the appropriate service from the Windows Services list and select the action to perform.

Power Center uses Network Service account to start all the services. You can change to a normal Windows OS user account for security purpose. For more information on how to change the account, see "Starting Services with a Normal Windows OS User Account" in the "Security" chapter.

Uninstalling Power Center

NOTE: After uninstalling Power Center, the existing power cap value set in the policies (including EPR) still remain effective on the devices. To avoid impacts to the devices, remove all devices from the Power Center management console before uninstalling Power Center. Make sure to check your data center power capacity before removing the devices to avoid tripping the breaker because the policies will be removed at the same time.

To uninstall Power Center:

1. Go to **Start** → **Control Panel** → **Add/Remove Programs**.
2. From the Add/Remove Programs dialog, select **Dell Power Measurement, Mitigation, and Management**, and click **Remove**.
3. Click **Yes** to confirm. Follow the on-screen instructions.

If you did not check the option "Use another database server" during the installation, the uninstall program removes the Power Center database and configurations.

If you checked the option "Use another database server" and used another database during the installation, the uninstall program does not uninstall the database.

Launching Power Center

To launch the Power Center management console, enter the following address in lower case in your Web browser: https://<*Server_Name*>:<*HTTPS_Port*>/powercenter/.

For example: https://localhost:8643/powercenter/.

NOTE: For Windows 2003, if you reinstall Power Center on the same server using a different HTTPS port, you must log off Windows OS then log in once to make sure the new HTTPS port takes effect.

NOTE: Power Center only supports screen resolutions of 1024*768 pixels or higher. Make sure you have correctly set the screen resolution on your system before launching the Power Center management console.

Configuring ESC for Internet Explorer

If the Power Center server uses Windows 2003 Server or Windows 2008 OS, and the Web browser is Internet Explorer 8 or version above, by default, the system has the Internet Explorer Enhanced Security Configuration (ESC) feature enabled. To make sure Power Center functions properly in Internet Explorer, you must either disable this feature or configure Internet Explorer to trust the Power Center site/links.

To disable this feature in Windows 2008:

1. Go to **Control Panel** → **System and Security** → **Administrative Tools** → **Server Manager**.
2. In the **Server Summary** → **Security Information** section, click **Configure IE ESC**.
3. The **Internet Explorer Enhanced Security Configuration** window opens, set enhanced security configuration to **Off** for both administrators and users.

To disable this feature in Windows 2003 Server:

1. Go to **Control Panel** → **Add or Remove Programs** → **Add/Remove Windows Components**.
2. Uncheck the **Internet Explorer Enhanced Security Configuration** check box.
3. Click **Next**, and then click **Finish**.

To trust the Power Center site/links:

1. Go to **Internet Explorer** → **Tools** → **Internet Options** → **Security**.
2. Click **Trusted Sites**, add **about: Blank** in trusted sites.

NOTE: You may need to restart Internet Explorer for the configuration to take effect.

4

Access Control

This chapter provides information about the access control in Power Center, including:

- Log in/Log out — You can log into Power Center by entering a user account or by Kerberos Single Sign-On (SSO).
- User/Role/Privilege Management — After you have logged in, you can manage user accounts in the management console. Power Center provides role-based access control. You must set up roles first, and define the privileges for each role. After that, you can set up Power Center accounts and assign them with different roles.
- Licensing — Power Center requires a valid license. You must import a license before the trial license expires.

About Authentication

Power Center supports Power Center managed users and Windows users.

For cross-domain authentication, the domains must be two-way transitively trusted by the domain in which the Power Center server is installed.

For domains that are one-way trusted or not trusted by the domain in which the Power Center server is installed, the authentication of user accounts in these domains is not supported and may fail.

Logging in

About Login

Power Center supports the following login methods:

- Log in with user name and password — You can use your user account to log into Power Center. For more information, see "Log in with User Name and Password" in this chapter.
- Log in using Kerberos Single Sign-On (SSO) — This feature enables you to log in without entering the user name and password if you have already logged in the Windows domain with your domain account. Power Center

only supports Kerberos-based SSO. For more information on SSO, see "Single Domain Environment" and "Multiple Domain Environment" in this chapter.

NOTE: You cannot log into Power Center locally using SSO, i.e., you cannot log into Power Center using SSO on the Power Center server. You only can log into Power Center using SSO remotely.

NOTE: You must add the SSO user account to Power Center before you can log in using SSO. You will skip the login page and enter the **Getting Started** page directly using SSO. After you log into Power Center, you cannot log out when you click **Logout**. To log out, close the Web browser or Power Center management console.

Power Center tries Kerberos SSO first. If it fails, the Power Center login form appears and you can use the user account information to log into Power Center.

Log in with User Name and Password

To log into Power Center with the user name and password, you can use one of the following accounts:

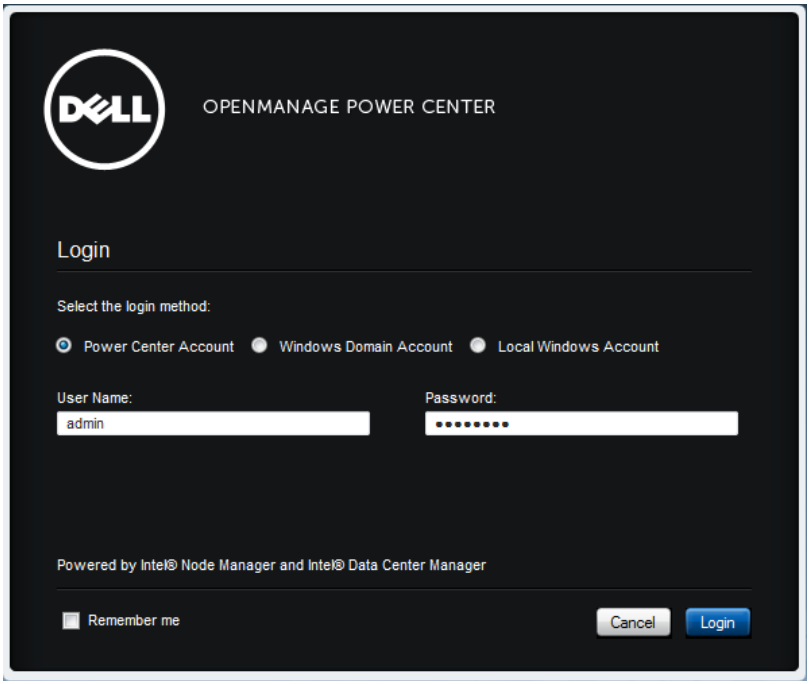
- Power Center Account — You can create this account in Power Center. For the first-time login, you must use the Power Center user account created during the installation.
- Domain Account — Windows domain account.
- Local Windows Account — Windows local account on the Power Center server.

NOTE: Before logging into Power Center using either the Windows domain or the Windows local account, you must add the account into Power Center by accessing the **User Accounts** page.

For more information on how to open the Power Center management console, see "Launching Power Center" in the "Installing and Launching" chapter.

Log in Using Your Power Center Account

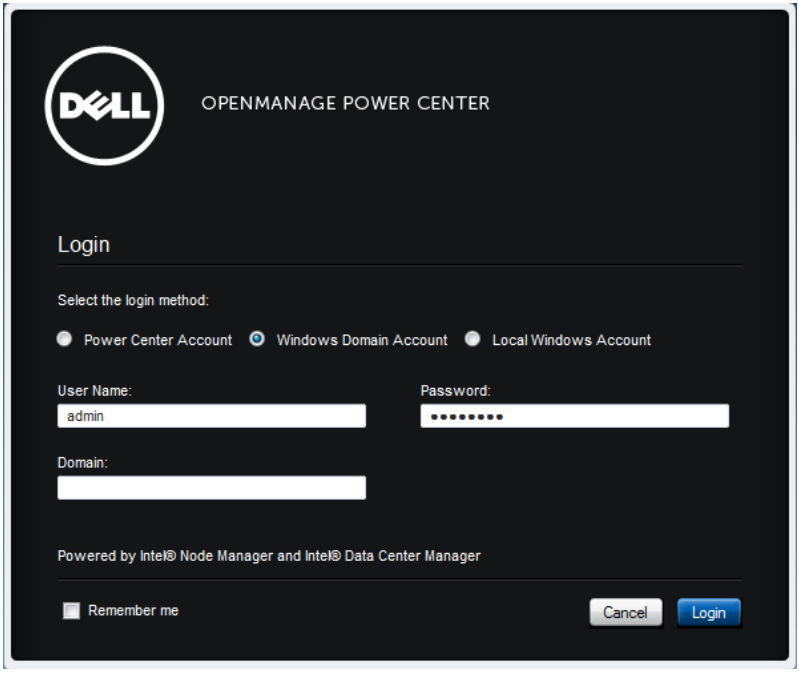
To log in using your Power Center Account:



1. Select **Power Center Account** (default).
2. Enter the **User Name**. This is the user name of the Power Center account.
3. Enter the **Password**. This is the user password of the Power Center account.
4. Click **Login**.

Log in Using the Windows Domain Account

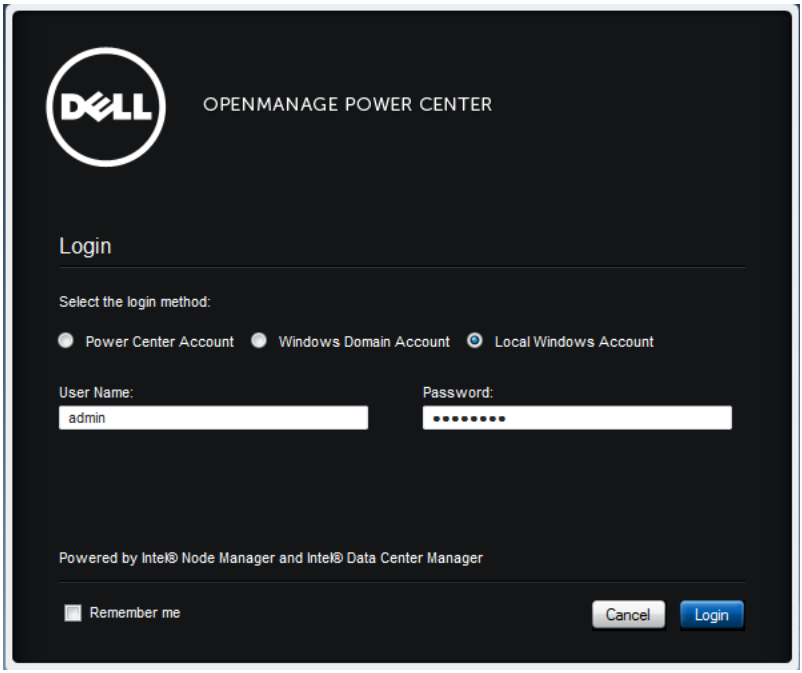
To log in using the Windows Domain Account:



1. Select **Windows Domain Account**.
2. Enter the **User Name**. This is the user name of the Windows domain account.
3. Enter the **Password**. This is the user password of the Windows domain account.
4. Enter the **Domain**. This is the domain name of this user account.
5. Click **Login**.

Log in Using the Windows Local Account

To log in using the Windows Local Account:



1. Select **Local Windows Account**.
2. Enter the **User Name**. This is the user name of the local Windows account.
3. Enter the **Password**. This is the user password of the local Windows account.
4. Click **Login**.

After successful login, the **Getting Started** page opens. Now you can start to use Power Center functions.

NOTE: A windows local account with blank password may fail to log into Power Center due to the Windows security policy settings. For more information on the security policy settings, see the Microsoft Web site or Windows Help.

Log in with Single Sign-on (SSO)

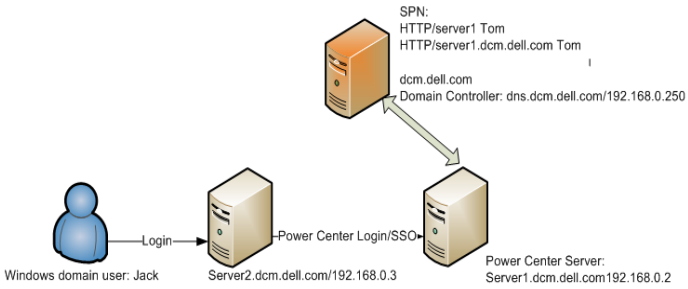
SSO uses centralized authentication servers that other applications and systems utilize for authentication purposes, and combines this with techniques to ensure that users do not actively have to enter their credentials more than once.

Kerberos SSO requires specific domain environment settings for the Windows Active Directory (AD) domain controller, Power Center server, and Web browser.

Single Domain Environment

The following illustration shows how to set up a single domain environment with the following components:

- Domain Controller — dns.dcm.dell.com is the Windows AD server that supports domain dcm.dell.com (Father and Child).
- Power Center Server — server1.dcm.dell.com is the server with Power Center installed.
- Power Center Client — server2.dcm.dell.com is the client server that connects to the Power Center server.



To set up the Kerberos SSO single domain environment, perform the following steps:

Step 1. Install Power Center

When installing Power Center:

1 Set up a Realm Name. You must enter a Fully Qualified Domain Name (FQDN) of the Realm. For example, dcm.dell.com.

2. Set up AD domain controller addresses. Separate multiple addresses with a comma. For example, 192.168.0.250.
3. Specify a domain user for dcm.dell.com as Power Center server's domain account for Kerberos SSO. This user account must be an existing and valid domain user account. For example, "Tom" and Tom's password.

Step 2. Set up Service Principle Name (SPN) for Power Center service in AD Domain Controller

1. Log into the AD domain controller as an Administrator.
2. Open a command console.
3. Add two SPNs for Power Center, use server FQDN in one SPN and server NetBIOS name for the other SPN. The user account associated with service SPN must be the Power Center server's domain account for Kerberos SSO configured during Power Center installation or in the **Settings** page. For example:

```
setspn -a HTTP/server1.dcm.dell.com Tom

setspn -a HTTP/server1 Tom
```

Step 3. Configure Web browser

You must configure your Web browser to support SSO. For more information on how to configure this, see your Web browser Help. For a list of supported Web browsers, see "System Requirements" in the "Overview" chapter.

NOTE: To correctly set up Kerberos SSO: 1) The date and time on all involved computers must be consistent. 2) DNS configuration must be correct.

To support SSO in Firefox, you must send Kerberos credentials to the appropriate KDC.

To support SSO in Internet Explorer, you must add the Power Center server as a local Intranet site.

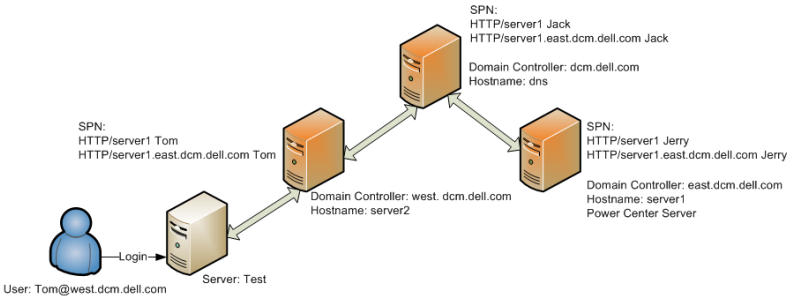
The following is an example of configuration steps in Microsoft Internet Explorer 8:

1. Go to **Internet Explorer** 8 → **Internet Options** → **Security** → **Local Intranet,** and click **Sites**. The Local Intranet window opens.
2. Click **Advanced**, add your Power Center site into Local Intranet. For example, server1.dcm.dell.com.

Multiple Domain Environment

The following illustration shows how to set up a multiple domain environment with the following components:

- Domain Controller — There are several Windows AD domain controllers in the illustration, including the parent domain dcm.dell.com and the child domans east.dcm.dell.com and west.dcm.dell.com.
- Power Center Server — server1.east.dcm.dell.com is the server with Power Center installed. It is an AD domain controller, the domain name is east.dcm.dell.com。
- Power Center Client — test.west.dcm.dell.com is the client server that connects to the network of the Power Center server.



To set up the Kerberos SSO multiple domain environment, perform the following steps:

Step 1. Install Power Center

When installing Power Center, do the following:

1. Set up the Default Realm Name of the domain in which Power Center is installed. You must enter FQDN. For example, east.dcm.dell.com.
2. Set up the AD Domain Controller addresses. Separate multiple addresses with a comma. For example, 192.168.0.2, 192.168.0.3.
3. Specify a domain user for east.dcm.dell.com as Power Center server's domain account for Kerberos SSO. For example, "Jerry" and Jerry's password.

Step 2. Set up SPN for Power Center service

Set up SPN for Power Center service in all involved AD domain controllers. In the example, three domains are involved: dcm.dell.com, east.dcm.dell.com and west.dcm.dell.com. Repeat the following steps on each domain.

1. Log into the AD domain controller as an Administrator.
2. Open a command console.
3. Add two SPNs for Power Center:
   - If it is on the Default Realm (configured in Step 1), the user account associated with the service SPN must be the Power Center server's domain account for Kerberos SSO configured in Step 1. For example,

     ```
     setspn -a HTTP/server1.east.dcm.dell.com Jerry
     ```

     ```
     setspn -a HTTP/server1 Jerry
     ```

   - If it is not on the Default Realm, for example, it is on dcm.dell.com, the user account associated with the service SPN must be a domain user account in the current domain. For example, Jack is a domain user in dcm.dell.com. Use the following commands to create service SPN on the dcm.dell.com domain controller.

     ```
     setspn -a HTTP/server1.east.dcm.dell.com Jack
     ```

     ```
     setspn -a HTTP/server1 Jack
     ```

Step 3. Configure Web browser

You must configure your Web browser to support SSO. For more information on the configuration, see step 3 of "Single Domain Environment" in this chapter.

Windows NT LAN Manager (NTLM) Authentication Limitation

Power Center supports Kerberos SSO for Windows domain user authentication. To enable this feature, Power Center is configured to support the Windows integrated authentication option which includes two authentication mechanisms: Kerberos and NTLM .

NTLM is not supported in Power Center. If the client's Web browser uses NTLM to authenticate domain users for Power Center, there are some limitations.

What's the limitation?

The Web browser displays a message box requiring a Windows user name and password:

- If you press **OK** after entering a user name and password, whether the information is correct or not, the Power Center login page appears and requires you to authenticate through the login page.
- If you press **Cancel**, there is an HTTP Status 401 failure and you cannot log into Power Center.

When does this occur?

When one of the following elements of Kerberos SSO is not correctly configured: Power Center server, Web browser or AD domain controller configuration.

How to solve?

Correctly configure your Power Center server, AD controller and Web browser for Kerberos SSO. For more information on how to configure, see the section above and your Web browser Help.

Multiple User Login

Power Center supports up to ten concurrent user login instances. When multiple users log into Power Center, if one user implements a change in Power Center, for example, deleting a device or moving a device, this may cause unexpected behavior for other logged in users. For example:

- If another user is viewing the pages, this user may see inconsistent data.
- If another user is performing operations on the same device, this user may receive an error message.

Logging out

You can log out of Power Center after completing your tasks.

To log out of Power Center, click **Logout** at the upper right corner of the management console.

Managing User Roles

Power Center supports three types of pre-defined roles. Each role has different privileges:

- Administrator — All privileges.
- Power User — All privileges except the "Manage Role/User" and "Manage License" privileges.
- Guest — "View Device/Group" privileges only.

Only a user with the "Manage Role/User" privilege can add/edit/delete a role in Power Center.

Adding a Role

If you are an administrator, you can add a new role, assign privileges to it, and add users to the new role.

To add a role:

1. Go to **Settings** → **User Accounts** → **User Roles**, and click **Add Role**.
2. Enter the following role information:
   - Name — Role name. The length must be less than 50 characters. The role name must be unique.
   - Description — Optional. Role description. The length must be less than 1024 characters.
   - Privileges — Select the privileges for this role.
3. Click **Apply**.

Updating a Role

To update a role:

1. Go to **Settings** → **User Accounts** → **User Roles**, and click **Edit**.
2. Edit the role name, description, or privileges.
3. Click **Apply**.

NOTE: Pre-defined roles cannot be edited.

Deleting a Role

To delete a role:

1. Go to **Settings** → **User Accounts** → **User Roles**, and click **Delete**.
2. Select the roles' checkboxes to delete them.
3. Click **Apply**.

NOTE: Pre-defined roles cannot be deleted.

Managing User Accounts

You can create users and assign them with different roles.

If you have the "Manage Role/User" privilege, you can add/edit/delete a user in Power Center.

Adding a User

If you have the "Manage Role/User" privilege, you can add a new user and assign roles to this user.

To add a user:

1. Go to **Settings** → **User Accounts** → **User Accounts**, and click **Add User**.
2. Select the user type. Enter the required information:

- **Local Windows Account** — Enter a valid user name of the Windows account. It can be either a user account name or a group account name.
- **Windows Domain Account** — Enter a valid user name of the Windows domain account and Windows domain name. It can be either a user account name or a group account name.

- **Power Center Account** — Create a user name and password for the Power Center account. For more information on the user name and password rules, see Step 8 of "Installing Power Center" in the "Installing and Launching" chapter.

3 Select the user roles. You can select multiple (0-4) roles to assign more privileges for the user.

NOTE: If you assign user A to role 1 and role 2, it has all privileges of role 1 and role 2.

4 Enter the user description. This field is optional. This is useful when there are two users with the same user name. You can enter a description to distinguish between them.

5 Click **Apply**.

Updating a User

After a user is created, you can update the user's privilege or password; however, you cannot update the user type and description.

To update a user:

1 Go to **Settings** → **User Accounts** → **User Accounts**.

2 Click **Update Password** to update the user password, or click **Edit** to edit Role 1, Role 2, Role 3, or Role 4 to update user privileges.

3 Click **Apply**.

NOTE: You cannot edit the privileges of the Power Center super user that was created during the installation.

Deleting a User

To delete a user:

1 Go to **Settings** → **User Accounts** → **User Accounts**, and click **Delete**.

2 Select the users' checkboxes to delete them.

3 Click **Apply**.

NOTE: You cannot delete the Power Center managed user (super user) that was created during the installation.

Managing Privileges

A user privilege is a right to execute a particular type of Power Center function. Privileges are not configurable, however you can configure roles, which group several privileges together.

Power Center has the following pre-defined privileges for each role:

- Global configuration
- Device discovery
- Manage role/user
- View device/group
- Manage device/group
- Manage policy
- Manage event
- Manage license

Each page in the Power Center management console can function differently according to the user privilege:

- Fully functional — User can view and edit.
- Partially functional — User can partially view or edit.
- Not functional — User sees a blank page.

The following table lists the functional status of each page for the different user privileges.

Table 4-1. Pages and Privileges

Page	Privilege and Page Status
Getting Started	**Fully functional:** All users. **Partially functional:** NA **Not functional:** NA

Table 4-1. Pages and Privileges

Page	Privilege and Page Status
Power Overview	**Fully functional:** For users with the "Manage Device/Group," "View Device/Group," "Manage Event" and "Manage Policy" privileges. **Partially functional:** Users with only "View Device/Group" and "Manage Policy" privileges cannot view Thresholds tab. Users with only "View Device/Group" and "Manage Event" privileges cannot view Policies tab. **Not functional:** For users without the "View Device/Group" privilege.
Group Management	**Fully functional:** For users with the "Manage Device/Group" privilege. **Partially functional:** NA **Not functional:** For users without the "Manage Device/Group" privilege.
Discovery	**Fully functional:** For users with the "Device Discovery" privilege. **Partially functional:** NA **Not functional:** For users without the "Device Discovery" privilege.

Table 4-1. Pages and Privileges

Page	Privilege and Page Status
Device List	**Fully functional:** For users with the "View Device/Group" and "Manage Device/Group" privileges. **Partially functional:** Users with the "View Device/Group" privilege can view devices on this page. **Not functional:** Users without the "Manage Device" and "View Devices/Group" privileges will see a blank page.
Policies	**Fully functional:** For users with the "View Device/Group" and "Manage Policy" privileges. **Partially functional:** NA **Not functional:** Users without the "View Device/Group" and "Manage Policy" privileges will see a blank page.
Compare	**Fully functional:** For users with the "View Device/Group" privilege. **Partially functional:** NA **Not functional:** For users without the "View Device/Group" privilege.
Settings → Settings	**Fully functional:** For users with the "Global Configuration" privilege. **Partially functional:** Users without the "Global Configuration" privilege can only view part of the settings on this page. **Not functional:** NA

Table 4-1. Pages and Privileges

Page	Privilege and Page Status
Settings → User Accounts	**Fully functional:**
	For users with the "Manage Role/User" privilege.
	Partially functional:
	Users without the "Manage Role/User" privilege only can view their own user information.
	Not functional:
	NA
Settings → Licensing	**Fully functional:**
	For users with the "Manage License" privilege.
	Partially functional:
	Users without the "Manage License" privilege only can view the license information.
	Not functional:
	NA
Event Logs	**Fully functional:**
	For users with the "Manage Event" and "View Device/Group" privileges.
	Partially functional:
	Users with the "View Device/Group" privilege only can view the events on this page.
	Not functional:
	NA

Global Configuration

The "Global Configuration" privilege enables:

- Changing the Power Center global configuration. For example, you can configure the sampling interval or database settings.

What happens without this privilege?

You only can view part of the **Settings** page, you cannot make any changes. There is no Edit option.

Device Discovery

The "Device Discovery" privilege enables:

- Discovering network devices

What happens without this privilege?

You cannot see the **Power Overview** page in Power Center. You can view the **Settings** page, but cannot make any changes.

Manage Role/User

The "Manage Role/User" privilege enables:

- Creating role
- Deleting role
- Updating role
- Creating user
- Deleting user
- Updating user

What happens without this privilege?

You only can view your own user account information and update the password. The **User Roles** and **User Accounts** sections are not displayed in the **User Accounts** page.

View Device/Group

The "View Device/Group" privilege enables:

- Viewing all devices and groups information

What happens without this privilege?

You cannot view any device or group information; you can only view the **Settings** page.

NOTE: Users with only "View Device/Group" privilege have the following restrictions: 1) The **Discovery** page is not available to them. 2) The pages under **Devices Groups** do not enable Add/Delete/Edit functionalities.

Manage Device/Group

The "Manage Device/Group" privilege enables:

- Creating logical groups
- Creating a Data Center/Room/Aisle/Rack/Device
- Associating Data Center/Room/Aisle/Rack/Device/Logical Group with parent logical groups
- Deleting a Data Center/Room/Aisle/Rack/Device/Logical Group
- Managing a device
- Removing a device/group from the Device List

NOTE: When you assign the "Manage Device/Group" privilege to a user, Power Center automatically assigns the "View Device/Group" privilege to this user.

What happens without this privilege?

You can view all devices and groups information, but cannot add/delete/edit/manage the devices and groups.

Manage Policy

The "Manage Policy" privilege enables:

- Adding/removing a policy
- Updating a policy
- Starting/stopping Emergency Power Reduction on a device/group

NOTE: To manage a policy, you must also have the "View Device/Group" privilege.

What happens without this privilege?

You cannot see the **Policies** tab in the **Power Overview** page.

Manage Event

The "Manage Event" privilege enables:

- Adding/Removing an event condition (threshold)
- Updating an event condition (threshold)
- Removing an event

NOTE: To manage event, you must also have the "View Device/Group" privilege.

What happens without this privilege?

You can view the events information and add comment to the events, but cannot delete events. You cannot see the **Thresholds** tab in the **Power Overview** page.

Manage License

The "Manage License" privilege enables:

- Importing a license

What happens without this privilege?

You only can view the License information, but the **Import License** option is not available.

Viewing Current User Information

You can click the login user name at the upper-right corner of any page, or go to **Settings → User Accounts → Current User** to view and update the current user information. You can:

- View the current user information
- Update the current user password

To update the user password:

1. Click **Update Password**.
2. Enter the current password and new password. Enter the new password again to confirm.
3. Click **Apply**.

Licensing

Power Center requires a valid license. You can import and view a license in the **Licensing** page.

Importing License

Power Center automatically installs a 60-day trial license during installation. When the trial license expires, most of the Power Center features are disabled. You must import a perpetual license before the trial license expires.

NOTE: Only users with the "Manage License" privilege can import a license.

To import a license:

1. Request a license from **www.dell.com/powercenter.**
2. Click **Import License**.
3. Click **Upload File**.
4. Select a license file, and click **Open**.

Power Center imports the license and brings up a message upon successful import. You can view the license information in the **Licensing** page.

Viewing License

Power Center license information includes:

- Product Name — Product name.
- Version — Product version.
- License Type — Trial (60 days) or Perpetual.
- Expiration — For Trial license only. Displays the license expiration date in the format: YYYY-MM-DD, Days Left: xx.
- Status — Valid or Expired.

NOTE: The **Getting Started** page displays a warning message when the license expires in less than 30 days.

5

Device Discovery

To manage devices in Power Center, you must add the devices to the Power Center management console first. You can add devices by discovering devices from the network, or adding devices manually.

This chapter explains how to discover devices from the network and add devices manually in the Power Center management console.

Power Center device discovery includes both the automatic detection of all devices on your data center and the collection of basic information about each device, such as the device name, connection status, device type, device model, its IP address and hostname, and the protocol it uses for communication. This enables you to track the device status and your data center information. You can also manage these discovered devices in Power Center. If there is a new or changed device in your data center, you can use the device discovery function to rediscover the devices.

You must have the "Manage Device/Group" and "Discover Device" privileges to add a device to Power Center.

There are two scenarios for adding devices:

- Add a device from the network — You can discover a device from the network. The discovered devices will be automatically added to the Device List.
- Add a device manually — You can use the Power Center management console to specify device properties and add a device to the Device List.

NOTE: If you use a network security policy, the discovery function may not work properly.

Supported Devices and Unsupported Devices

You can add or discover supported devices, and create a group structure to build out the data center. Power Center cannot discover or manage all device types, and unsupported devices must be added manually to make the data center group structure complete.

For supported devices:

- Device types include server, UPS, PDU and chassis.
- Set the connection protocol and credential information so that the device can communicate with Power Center.
- Add or discover a supported device to the Device List. Perform management functions including discovery, adding to the group structure, monitoring power and temperature, applying power management policies, and sending events.

For unsupported devices:

- Power Center does not communicate with unsupported devices, therefore connection protocol and credential information is not necessary.
- Unsupported devices cannot be discovered, only added manually to the Device List.
- Power Center adds the unsupported device to the group structure, but cannot manage it using the available management functions.

You may need to enter the following power values when adding supported or unsupported devices:

- **Faceplate Power:** The maximum amount of power that a group/device can draw; this value should be listed on the power supply specifications. The faceplate power rating is typically much higher than the actual power used by the device.
- **De-rated Power:** The default maximum power value; if a power measurement cannot be completed, this value is used.

  NOTE: Faceplate power value is always greater than the de-rated power value.

Adding a Device from the Network

This section explains how to use the Power Center management console to discover a device from the network.

Before adding a device from the network, make sure the DNS server is set up correctly. Specifically, make sure that:

- There is a DNS server running on the Power Center's network.
- The specified DNS server has a reverse DNS zone for the network on which you are trying to discover the devices.

NOTE: Power Center server tries to get device names from the DNS server specified in the network configuration of the operating system. This may cause the device name to be different from the actual one if the DNS server resolves the device IP address to a different device name.

To discover devices from the network, complete the following steps:

Step 1. Enter IP Range

1. Go to the **Discovery** page.
2. Enter the IP address range, or select one in the list. If the correct range is not displayed, add it using the following steps:
3. Click **Add IP Range**, and enter information in the following fields:
   - Beginning — The beginning IP address. For example, 192.168.1.1.
   - End — The end IP address. For example, 192.168.1.255.
   - Network Mask — The network mask. For example, 255.255.255.0.
4. Click **Apply**. The new IP range is added to the list of IP ranges and displayed at top of the page.
5. Select at least one IP Range, and click **Next**.

NOTE: The IP Ranges section lists not only the IP ranges that you have added, but also the IP ranges of the recent three discovery tasks.

Step 2. Select Protocol

You can either create a new protocol profile or use an existing protocol profile.

To create a new protocol profile:

1. Click **Add Protocol**.

   Enter information in the following fields:

   - Profile Name — Enter the profile name. The profile name must be less than 16 characters.
   - Description — Enter the description for this profile.
   - Protocol — Select the protocol used for communicating with devices through the network. You must enter credential information for the selected protocol. For more information on protocol information, see "Protocol Profile" in this chapter.
2. Click **Apply**. The new protocol profile is added and displayed at top of the page. Click + next to a profile to see its details.

3 Select the connnection protocol(s), and click **Next**.

Step 3. View Summary and Search Devices

1 The **Summary** information displays. Review the information and click **Search**.

2 After the search progress completes, go to the **Device List** page to validate that the correct devices are listed on the page.

You can also perform the following tasks related to the device discovery:

To edit an IP range:

1 Click **Edit**.

2 Enter the new IP range.

3 Click **Apply**. The IP address range is updated.

To view an active search:

1 Click **View Active Searches** to view the status of the active searches.

2 The search progress percentage bar displays and the bar automatically disappears when the search completes.

To view the recent discovery jobs:

1 The **Recent Discovery Jobs** section displays the four most recent discovery searches.

2 Click **Details** to view the history information on each search.

To rerun the search:

1 In the **Recent Discovery Jobs** section, click **Rerun Search** next to a discovery job.

2 The search starts automatically using the discovery job search criteria, and the device information is updated in the **Device List** page.

Adding a Device Manually

This section explains how to add a device manually in the Power Center management console.

To add a device manually:

1 Go to the **Device List** page, and click **Add**.

2 Enter the device and protocol information - Required Device Information, Protocol Information, Optional Device Information - for the device you want to add.

- **Required Device Information:**
  - Device Name: Enter the name of the device.
  - Device Type: Select a device type which includes Server, UPS, PDU, Chassis, or Unsupported.
  - IP Address or Hostname: Enter a valid IP address or hostname; optional for an Unsupported device.

  NOTE: Enter either the IP Address or the Host Name field, not both. Power Center will check its validation; make sure you have entered a valid IP address or host name.

- **Protocol Information:** Not required for an unsupported device. For more information on credential information for the protocols, see "Protocol Profile" in this chapter.
  - Protocol: The corresponding protocol type displays after you select the device type. If you selected a UPS or a PDU in the previous step, you must select a protocol.
  - Credential Information: Enter the protocol credential information.
- **Optional Device Information:**
  - Device Model: Enter the device model. This field is available when you add an unsupported device.
  - Size of Device: Select the device height: 1-10 rack unit.
  - Description: Enter a description for the device.
  - Faceplate Power: Enter the faceplate power value.
  - De-rated Power: Enter the de-rated power value.

3 Click **Apply**.

Rediscovering Devices in a Chassis

If you have physically added, removed or changed your devices in a chassis, you can update the device information:

1. Go to **Group Management** → **Physical (Logical) Group** → **View All Physical Groups**.
2. Click the selected physical/logical group icon and its device/group, and go to the Chassis level.
3. Click **Rediscover Chassis Devices**.

The devices information in the chassis is automatically updated.

Protocol Profile

Power Center server uses protocol profile to communicate with the devices by specifying the device connection protocol and credential information. You can add a new profile, edit an existing profile, or delete a profile. You can select a protocol profile to discover the devices.

Power Center supports the following connection protocol types, and includes several optional settings:

NOTE: Get the correct protocol type and credential information from your device administrator. The user name and password for the IPMI/WS-MAN protocol must be the same as those used for the iDRAC/CMC web console.

- IPMI: Select IPMI protocol for the server.
  - IPMI User Name — Maximum length is 16 characters.
  - IPMI Password — Maximum length is 255 characters.
  - IPMI Key — A string of 40 hex digits.
- WS-MAN: Select WS-MAN protocol for the chassis.
  - WS-MAN User Name — HTTP basic user name, maximum length is 255 characters.
  - WS-MAN Password — HTTP basic password, maximum length is 255 characters.
  - WS-MAN Port — Default value is 443, or enter a port number from 1 to 65535.
  - WS-MAN Validate Certificate — Optional. Enables device certificate validation.

    NOTE: A trusted certificate must be imported into the system before the WS-MAN Validate Certificate option is enabled or the communication may fail. For more information on how to install the certificate using the Dell Chassis

Management Controller, see "Configuration - New SSL Server Certificate Configuration" in the *Using Windows Remote Management (WinRM) to Remotely Manage Dell PowerEdge M1000e Using the Chassis Management Controller (CMC)* technical whitepaper. It can be downloaded from **http://www.delltechcenter.com/page/dcim.modular.cmc.winrm**. For more information on how to import the certificate to Power Center, see "Managing Certificates" in the "Security" chapter.

- SNMP v1v2c: Select an SNMP protocol version from SMMPv1, or SNMP v2/v2c for the PDU or UPS.
  - SNMP Community string — Required. Maximum length is 255 characters.
- SNMP v3: Select SNMP v3 for the PDU or UPS.
  - SNMP User Name — Required. Maximum length is 255 characters.
  - SNMP Authentication Password — Required. Maximum length is 16 characters.
  - SNMP Encryption Password — Maximum length is 255 characters. When the SNMP Authentication Password is empty, the SNMP Encryption Password is also empty.

You can set up multiple protocol profiles for each protocol.

6

Device Management

The **Device List** page lists network-discovered devices and devices added manually. From this page, you can:

- Add supported or unsupported devices to the **Device List** page
- Remove devices from the **Device List** page
- Edit device information for a single device or multiple devices
- Edit protocol information for a single device
- Filter and sort devices to meet current needs

Viewing Devices

The **Device List** page lists the following device information:

Table 6-1. Device Information

Field	Description
Name	Device Name. Power Center resolves this name during the network discovery.
Status	Device status, including: • Connected • Lost connection • Unknown
IP Address	Device IP address.
Hostname	Device hostname.
Serial Number or Service Tag	Device serial number or service tag. • Service Tag: The service tag for Dell chassis and servers is displayed. • Serial Number: The serial number for Dell PDU and UPS is displayed. • NA: For all other devices, NA is displayed.

Table 6-1. Device Information

Field	Description
Device Type	Device type, including: • Server • PDU • UPS • Chassis • Unsupported
Device Model	Device model, for example, PowerEdge M610.
Protocol	The protocol used for communication, including: • IPMI • SNMPv1v2c or SNMPv3 • WS-MAN
Power Capability	The power monitoring and capping capability, or if the device can be upgraded, including: • Unknown • None • Monitor • Monitor & Capping • Monitor and Upgradable
Group	The devices' physical group.
Time of Discovery	The time when the device was discovered.
Description	Device description.
Size of Device	The physical size of device, in rack units (U).
Faceplate Power	Device faceplate power.
De-rated Power	Device de-rated power.

NOTE: If a device is already discovered and listed in the **Device List** page, when Power Center runs a discovery task and this device is discovered again, all the device information for this device is updated in the **Device List** page. For more information on device discovery, see "Adding a Device from the Network" in the "Device Discovery" chapter.

Editing Devices

You can edit the device information of devices listed in the Power Center management console.

To edit a single device:

1. Go to the **Device List** page.
2. Click **Edit Tasks** → **Edit**.
3. Edit the **Name**, **Description**, **IP Address** or **Host Name**, **Size of Device**, **Faceplate Power** or **de-rated Power** of the device.

   NOTE: You cannot edit the Faceplate Power and De-rated Power for a chassis.

   NOTE: For IP Address and Host Name fields, enter either the IP Address or the Host Name field, not both. If you edit the IP address, Power Center does not check its validation. If you edit the host name, Power Center does check its validation. Make sure you enter a valid host name. If you edit the host name to an integer in the range of 0-4294967295, the Power Center server uses the IP address which can be represented by this integer for device communication. For example, if you edit the host name to 3232235777, the Power Center server communicates with the device using IP address 192.168.1.1.
4. Click **Apply**.

You can use the batch edit function to edit the information of multiple devices at once.

To batch edit devices:

1. Go to the **Device List** page.
2. Click **Edit Tasks** → **Batch Edit**.
3. Select the devices' checkboxes to edit them, and click **Next**.
4. Enter the **Size**, **Faceplate Power**, **de-rated Power**, **Description** or **Protocol** for the devices.

NOTE: 1) If you selected devices with different protocol types, then you cannot edit the protocol information. 2) If you edit the protocol information and leave the **User Name** field empty, the user name remains unchanged. 3) If you select the **Clear** checkbox next to a field, the current value of this field is cleared. If you do not select the **Clear** checkbox and leave this field empty, the value remains unchanged.

5 Click **Apply**.

Editing Protocol

You can edit the communication protocol of the devices listed in the **Device List** page.

To edit a protocol:

1 Go to the **Device List** page.

2 Click the device protocol link that you want to edit in the **Protocol** column.

3 The Edit Protocol Information window opens. Enter the protocol details. You must enter credential information for the protocol. For more information on the protocol information, see "Protocol Profile" in this chapter.

NOTE: 1) If you select the Clear checkbox next to a field, the current value of this field is cleared. 2) If you do not select the Clear checkbox and leave the field empty, the value remains unchanged.

4 Click **Apply**.

Deleting Devices

If you want to manually remove a duplicated device, or you do not want to manage a device in Power Center, you can delete the device from the Device List page.

To delete a single device or multiple devices:

1 Go to the **Device List** page.

2 Click **Delete Tasks** → **Delete**.

3 Select the devices' checkboxes to delete them.

4 Click **Apply**.

To delete all devices:

1. Go to the **Device List** page.
2. Click **Delete Tasks** → **Delete All**.
3. Read the pop-up message, and click **Yes** to continue.

Filtering Devices

You can apply a filter to show only specific devices, for example, devices of a certain type.

To filter devices:

1. Go to the **Device List** page.
2. Click **Filter**.
3. The **Filter** window opens. Click a filtering option in the left pane - **IP Range**, **Date Range**, **Protocol**, **Status**, **Device Type/Model**, **Physical Group**, **Faceplate/De-rated Power, or Power Capability** - to display a specific filtering option window.
4. In the filtering option window, use the displayed information to select filtering options. You can use one or more options to filter devices.
   - **IP Range** — Enter the start and end IP address of devices.
   - **Date Range** — Enter the start and end date of device discovery. Enter the dates manually following this format <YYYY-MM-DD>, or select the dates from the calendar. Devices discovered from 00:00:00 of start date to 00:00:00 of the next day after the end date are displayed. For example, if you enter the filtering option 2011-01-01 as both start date and end date, all devices discovered between 00:00:00 of 2011-01-01 and 00:00:00 of 2011-01-02 are displayed.
   - **Protocol** — Select the protocols used for communication. You can select multiple protocols.
   - **Status** — Select device statuses. You can select multiple statuses.
   - **Device Type/Model** — Select the device type or device model. Device Model is the specific model information of a device type. For example, PowerEdge M610. All the models that currently exist in the **Device List** page are shown. If you selected both **Device Type** and **Device Model**, make sure the device type matches the device model. Otherwise, no result is shown.

- **Physical Group** — Select a physical group where the device is located. You can select any level of the physical group, including data center, room, aisle, rack, chassis.
- **Faceplate/De-rated Power** — Enter a faceplate or de-rated power range of devices.
- **Power Capability** — Select the power capability of the device. You can select multiple power capabilities.

5 Click **Apply**. The **Device List** page displays the filtered devices.

Sorting Devices

By default, in the **Device List** pages, the devices are listed by **Name** in alphabetical order (A-Z). To sort the list, click the Up or Down symbol next to the field to list the devices in ascending or descending order. The symbol of the current sorting field is displayed in orange.

7

Group Management

You can configure several devices as a group so that you can manage them.

Power Center enables you to create and organize your devices into two distinct types of groups:

- **Physical Group**

  A physical group is a group of groups/devices with a structure mapping that represents the actual physical layout.

  For more information on how to create and manage physical groups, see the "Physical Groups" chapter.

- **Logical Group**

  A logical group is a collection of groups and devices with a logical relation. A logical group does not need to map with the actual physical layout.

  For more information on how to create and manage logical groups, see the "Logical Groups" chapter.

Mapping Group Structure Information

Power Center supports group stucture mapping for Dell PowerEdge rack servers and tower servers. For more information on the specific models, see "Supported Devices" in the "Overview" chapter.

After you have created or updated the group structure, Power Center automatically updates the location information in the firmware of supported devices at the following mapping structure:

- Data Center — Data center and Room information in Power Center, format: <Data Center - Room>.
- Aisle — Aisle information in Power Center.
- Rack — Rack information in Power Center.
- Rack Slot — Rack slot information in Power Center.
- Chassis — Chassis information in Power Center (if applicable).

NOTE: To view the updated location information on supported device, you must 1) Make sure the device status is "Connected" in Power Center. 2) Wait a few minutes for the location information to be updated in the firmware of the device.

Finding a Group or Device

After the data center group structure is set up, you can find a group or device from the **Power Overview** or **Group Management** page:.

You can do the following in the **Power Overview** page:

- Find a physical group or device (excludes Unsupported devices).
- Find a logical group.
- View the event status. If there are critical or warning events in the group or device, an event icon is displayed next to the group/device icon. If the critical and warning events both exist, only the critical event icon is displayed.
- View the power details of the group/device. For more information on power details, see the "Power Monitoring" chapter.
- Click the **Manage Group** link on the top to enter the **Group Management** page of the selected group/device.

You can do the following in the **Group Management** page:

- Find a physical group.
- Find a logical group.
- Manage the selected group. For more information on how to manage the groups, see the other sections in this chapter.
- Click the **View Power Overview** link on the top to enter the **Power Overview** page and view the power details.

To find a physical group or device:

1. Go to **Power Overview** → **Select a Physical Group or Device**. Or, go to **Group Management** → **Select a Physical Group**.The page displays the data center physical group structure on the top.
2. Click the data center and its group icon to expand the group structure.
3. Select the group or device that you are looking for.

4 The page displays the selected group/device at the right, and displays the corresponding **Power Overview** or **Group Management** page of the selected group/device.

To find a logical group:

1 Go to **Power Overview** → **Select a Logical Group**. Or, go to **Group Management** → **Select a Logical Group**. The page displays the logical group list on the top.

2 Click a logical group icon to display its contents.

3 Select the group or device that you are looking for.

4 The page displays the selected group at the right, and displays the corresponding **Power Overview** or **Group Management** page of the selected group.

8

Physical Groups

A physical group is a group of groups/devices with a structure mapping that represents the actual physical layout.

As an IT/facility administrator, you may need to organize devices and groups according to their physical layout in the data center. Power Center enables you to monitor power/temperature information, manage policies/events at individual device, chassis, rack, aisle, room or data center levels.

Data Center Physical Group

Power Center manages physical groups with the following group structure:

Data Center → **Room** → **Aisle** → **Rack** → **Chassis**. You must create physical groups in this order.

PDU, UPS and unsupported devices can be attached at any level of the physical group structure. You can find the PDU and UPS devices information at the bottom of the group's page.

You can manually create physical groups, then add devices into the groups through the management console.

Creating Physical Group

To create a physical group:

1. Go to **Group Management** → **Physical Groups**, and click **Select a Physical Group**.
2. Click **Add New**.
3. Enter a **Name** and **Description** for the data center.
4. You can create multiple groups at once if you click **Add New <Entity Name>** in the **Tasks** section. Click **Duplicate Group** and enter the **Number** of the groups to create. Power Center automatically names the groups by adding a number (starting from 1) to it. For example, if you enter the name GroupA and number 10, Power Center creates ten groups named GroupA1, GroupA2 ...GroupA10.

5 Click **Apply**.

Managing Physical Groups

Adding Devices to a Physical Group

After you create a physical group, you can add or associate devices to this group.

To add/associate a device:

1 Click the physical group icon to open the Room Contents page. Click **Add New Room**, enter the Name and Description, and click **Apply**.

2 Click the room icon to open the Aisle Contents page. Click **Add New Aisle**, enter the Name and Description, and click **Apply**.

3 Click the aisle icon to open the Rack Contents page. Click **Add New Rack**, enter the Name, Description, Capacity (rack size) and Total Power Capacity (total rack power capacity), and click **Apply**.

NOTE: Rack power capacity is a field that indicates the physical power limitation in a rack; it is determined by the PDU capacity in power distribution topology of the data center. This field also sets the upper limit (ceiling) on the power policy that can be configured for the rack.

4 Click the rack icon to open the **Devices in Rack** page. The following devices are not displayed in the Device List when you add the devices to a rack.

- Blade servers.
- Devices without device size information. For example, a PDU or UPS, or a device that was manually added without the device information entered.
- A device whose size exceeds the continuous available slots on the rack.

You can add a device to a rack using the following options:

- **Add a device to a rack**
  - **a** Click **Devices in Rack** → **Add to Rack Slot**.
  - **b** Select a slot, and click **Add Devices to Selected Slot**.
  - **c** The **Add Device to Rack** window displays any devices that are not defined to a physical group. Use the following options to organize the device information:

- Show additional columns: The page displays three device information columns by default (Select, Name, Status). Click **Show Additional Columns** to display all columns.
- Filter: Use the filtering options to filter the devices.

d Click **Select** next to the devices to add, and click **Apply**. The selected devices are added to the selected slot and are displayed in the Device List.

NOTE: When the device size is greater than 1U and there are available slots on the top of the selected slot, Power Center automatically adds the devices to the rack. If slots are not available, adding the device fails and another slot will need to be selected.

NOTE: You cannot add or remove devices in a chassis; however, you can rediscover the devices in a chassis. For more information on how to rediscover devices, see "Rediscovering Devices in a Chassis" in the "Device Discovery" chapter.

- **Add devices to a rack in a batch**

a Click **Devices in Rack → Batch Add**.

b In the **Batch Add Devices to Rack** window, the devices that are not defined to any physical group are shown. You can also use the following options to display the device information to meet your needs:

- Show additional columns: By default, the page displays three columns of the device information (Select, Name, Status). You can click **Show Additional Columns** to display all columns of the device information.
- Filter: If you need to show only specific devices from a long list of the devices, you can use filtering options to filter the devices.

c Click **Select** next to the device that you want to add, and then select the slot for device by one of the following:

- Slot number: You can specify a slot number for the device. Power Center will add the device to this slot and the slots above it according to the device size.
- Auto: If you select **Auto**, Power Center will automatically assign slots for selected devices according to the device size and available slots. All selected devices are added to the rack.

d Repeat the previous step to select more devices and the corresponding slots. You can select multiple devices from different pages.

e Click **Apply**.

NOTE: If there are not enough slots available, the batch operation of adding devices to the rack will fail. You must re-select the devices and slots

- **Add associated devices to rack**

a Click **Devices Associated with Rack → Add to Rack**.

b In the **Associate a Device with a Rack** window, select the devices to add.

c Click **Apply**.

NOTE: Only PDU or UPS can be associated to the physical group.

5 The physical group is created and devices are added/associated to the group.

NOTE: One device can only exist in one physical location.

NOTE: When adding Dell Chassis Management Controller (CMC) to a physical group, if a blade server is found, you must manually update the credential of the blade server. Once you supply Power Center with the correct credential, Power Center updates its status from "lost connection" to "connected".

Editing Devices in a Physical Group

After adding or associating devices, you can edit the device information.

To edit a device, use one of the following:

- Click **Edit Tasks → Update Slots** to change the slot for the device.
- Click **Edit Tasks → Move** to move the device to other data center.
- Click **Edit Tasks → Edit** to edit the device.

Removing Devices from a Physical Group

To remove a device from the group:

1 Click **Remove**.

2 Select the devices' checkboxes to remove them.

3 Click **Apply**.

NOTE: After the device is removed, it still exists in the **Device List** page. You can add it to any physical group or logical group when needed.

Moving Devices in a Physical Group

You can move devices to update the group structure that is similar to the actual data center device structure when a device is moved physically in the data center.

A server or a chassis can only be moved to another rack. PDU, UPS and Unsupported devices can be moved to any level of the physical group structure.

NOTE: The blades are populated automatically to the chassis when the chassis is added to the rack. If the blades were not discovered when the chassis was added to the rack, the blades will be shown as Disconnected in the Device List. The status will be updated to Connected once the blades are discovered through the discovery process. When the blade is moved physically in the chassis or from one chassis to another, the Chassis group structure from the Power Center user interface will be updated only after the chassis is re-discovered through the Power Center discovery process.

To move a device:

1. Click **Move**.
2. The **Move Device** window displays the physical group structure of the device on top, and displays a list of physical groups (data center) under it as active links. If you move a device in the rack, click an active link to expand the group to display the racks, and then select the rack to which you want to move the device. If you move a device associated to a physical group, click an active link to select another group.
3. Click **Move**. The devices are moved to the selected rack or group.

Moving a Physical Group

You can move a physical group, and update the group structure so that it is similar to the actual data center device structure when a physical group is moved physically in the data center. The Physical Group can be a room, an aisle, or a rack.

You must move the physical group according to the following physical group structure: Data Center → Room → Aisle → Rack.

To move a physical group:

1. Click **Move**.
2. The **Move Physical Group** window displays the physical group structure of the physical group on top, and displays a list of physical groups (data center) under it as active links. Click an active link to expand the group to display all groups that are part of that physical group, and then select a group.
3. Click **Move**. The physical group is moved to the selected group.

Editing Physical Groups

After you have created a physical group, you can edit the group information to update it.

To edit the group information of a physical group:

1. Go to **Group Management** → **Physical Groups**, and click **Select a Physical Group**, then click the icons to select a group.
2. Click **Edit**.
3. Edit the **Name** and **Description** for the group.
4. Click **Apply**.

Deleting Physical Groups

To delete a physical group:

1. Go to **Group Management** → **Physical Groups**, and click **Select a Physical Group**, then click the icons to select a group.
2. Click **Delete**.
3. Select the groups' checkboxes to delete them.
4. Click **Apply**.

NOTE: If deleting the physical group affects the policy, an event will be sent. You can view it in the **Event Logs** page.

Viewing Physical Groups

To view details of the physical group, go to the **Physical Groups** page. There are two scenarios for accessing the **Physical Groups** page:

- Access from the left pane of the Power Center management console: You can click **Group Management → Select a Physical Group** to enter this page. This page lists all of the data centers. You can click a data center's active link to expand the contents.
- Access from the **Power Overview** page: You can click the **Manage Group** link on top of the **Power Overview** page to access the specific group/device content page. This page lists the detailed information of the content in this group/device.

The **Physical Groups** page lists all the physical groups by name in alphabetical order (A–Z). You can click a physical group's active link to view more details

- Group structure information —

  Click the icons to view the group structure, including Room, Aisle, Rack, Chassis.

- Group details —

  Click the tabs to view the details.

  – Events — Events in the group, including Critical, Warning events. For more information on event severity, see "Event Severity Levels" in the "Event Management" chapter.
  – Dashboards — Power dashboard and temperature dashboard.
  – Power Details — Power graphic and energy consumption summary.
  – Temperature Details — Temperature graphic and details summary.
  – Policies — The policies created for the physical group and their status.
  – Thresholds — Power thresholds and temperature thresholds.
  – Rack — The information of the devices in the rack. This tab appears when you view information at the Rack level.
  – Chassis — The information of the devices in the chassis. This tab appears when you view information at the Chassis level.

For more information on dashboards, power details, temperature details, policies, and thresholds, see the "Power Monitoring" and "Temperature Monitoring" chapters.

9

Logical Groups

A logical group is a collection of groups and devices with a logical relation. A logical group does not need to map with the actual physical layout. For example, there can be a logical group for all print file servers or email servers.

Creating a Logical Group

To create a logical group:

1. Go to **Power Overview** → **Logical Group**, and click **Select a Logical Group**.
2. Click **Add New Logical Group**.
3. Enter a **Name** and **Description** for the logical group.
4. You can create multiple groups at once if you click **Add New Logical Group**. Click **Duplicate Group** and enter the **Number** of the groups to create. Power Center automatically names the groups by adding a number (starting from 1) to it. For example, if you enter the name GroupA and number 10, Power Center creates ten groups named GroupA1, GroupA2 ...GroupA10.
5. Click **Apply**.

Managing Logical Groups

After you created a logical group, you can add a physical group, device, or another logical group to this group.

Adding a Logical Group

To add a logical group:

1. Click **Add New**.
2. Select the physical group, logical group, or device, and click **Apply**.

Adding Devices or Groups to a Logical Group

You can add devices or groups to a logical group. Only one device or group can be added at a time.

Add a device or group from one of the following categories:

- Physical Group
- Logical Group
- All Devices

NOTE: Chassis are not listed in the **All Devices** window; you cannot add a chassis to a logical group from the **All Devices** category. However, you can add a chassis from the **Physical Group** category if the chassis is already added to a rack.

To add a device or group to a logical group:

1. Click a category in the left pane - **Physical Group**, **Logical Group**, or **All Devices** - to display a specific group/device selection window.
2. In the selection window, use the displayed information to select a group or device.

- **Physical Group:**
  - **a** The group selection window lists the physical groups as active links. Click an active link to expand the group to display all groups that are part of that physical group.
  - **b** Click a physical group's active link, and then click **Select**.
  - **c** The physical group is added to, and displayed in, the **Group Management: Logical Groups** page.
- **Logical Group:**
  - **a** The group selection window lists the logical groups as active links.
  - **b** Click a logical group's active link.
  - **c** The logical group is added to, and displayed in, the **Group Management: Logical Groups** page.
- **All Devices:**
  - **a** The group selection window displays a list of all devices.
  - **b** Click **Select** to add the device to the **Group Management: Logical Groups** page.

Editing Logical Groups

After you created a logical group, you can edit the logical group information.

To edit a logical group:

1. Go to **Group Management** → **Logical Groups**, and click **Select a Logical Group**, then click the icons to select a group.
2. Click **Edit**.
3. Enter new **Name** and **Description** for the group.
4. Click **Apply**.

Deleting Logical Groups

To delete a logical group:

1. Go to **Group Management** → **Logical Groups**, and click **Select a Logical Group**, then click the icons to select a group.
2. Click **Delete**.
3. Select the groups' checkboxes to delete them.
4. Click **Apply**.

NOTE: If deleting the logical group affects the policy, an event will be sent. You can view it in the **Event Logs** page.

Viewing Logical Groups

To view details of the logical group, go to the **Logical Groups** page. There are two scenarios for accessing the **Logical Groups** page:

- Access from the left pane of the Power Center management console: You can click **Group Management** → **Select a Logical Group** to enter this page. This page lists all of the logical groups. You can click a logical group's active links to expand the contents.
- Access from the **Power Overview** page: You can click the **Manage Group** link on top of the **Power Overview** page to access the specific group's/device's content page. This page lists the detailed information of the content in this group/device.

The **Logical Groups** page lists all logical groups by name in alphabetical order (A-Z). You can click a logical group's active link to view more details:

- Group structure information —

  Click the icons to view the group structure, including physical group structure, logical group components, and devices that are directly under this logical group.

- Group details —

  Click the tabs to view the details.

  - Events — All events in the logical group, including Critical, Warning and Informative. For more information on event severity, see "Event Severity Levels" in the "Event Management" chapter.
  - Dashboards — Power dashboard, temperature dashboard and power capacity details (for racks only).
  - Power Details — Power graphic and energy consumption summary.
  - Temperature Details — Temperature graphic and details summary.
  - Policies — The policies applied on the logical group and their status.
  - Thresholds — Power thresholds and temperature thresholds.

For more information on dashboards, power details, temperature details, policies, and thresholds, see the "Power Monitoring" and "Temperature Monitoring" chapters.

10

Power Monitoring

Power Center enables the monitoring of current or historical power-related metrics (for example, power consumption or cost). This can help you understand the power status in the data center and plan for additional power infrastructure, cooling, and facility needs.

You can monitor power at different device/group levels, you can configure power monitoring settings to meet your monitoring needs, and you can also print the power status graph.

Power Monitoring Level

Power Center provides power monitoring at the following levels:

For physical groups and logical groups:

- Individual device
- Rack
- Aisle
- Room
- Data center

For logical groups only:

- User-defined logical group

Power Monitoring Configuration

You can configure power monitoring settings in Power Center, including:

- Thresholds (Average, maximum power for events)
- Device and group range (Monitor all or not)
- Sampling interval (1, 3, 6 minutes)
- Default units (Watts, or BTU per hour)
- Energy consumption (Power consumption and cost)

Thresholds is useful if you want to be notified when the power of the group/device exceeds the thresholds. Once the power value exceeds a critical or warning threshold, the related event is sent.

To configure thresholds:

1. Go to **Power Overview** → **Select a Physical Group or Device** or **Select a Logical Group**, and click the group/device icon.
2. Go to **Thresholds** → **Power Thresholds**, and click **Edit**.
3. Enter values for the following:

- Critical threshold for maximum power:

  When the maximum power exceeds the setting, the critical-level event "Max Power" is sent.

- Critical threshold for average power:

  When the average power exceeds the setting, the critical-level event "Average Power" is sent.

- Warning threshold for maximum power:

  When the maximum power exceeds the setting, the warning-level event "Max Power" is sent.

- Warning threshold for average power:

  When the average power exceeds the setting, a warning-level event "Average Power" is sent.

4. Click **Apply**.

After you configure the thresholds, you will see four lines with different colors indicating the thresholds in the **Power Details** tab.

For more information on how to configure device/group range and sampling interval, see "Monitoring Settings" in the "Configuring Power Center" chapter.

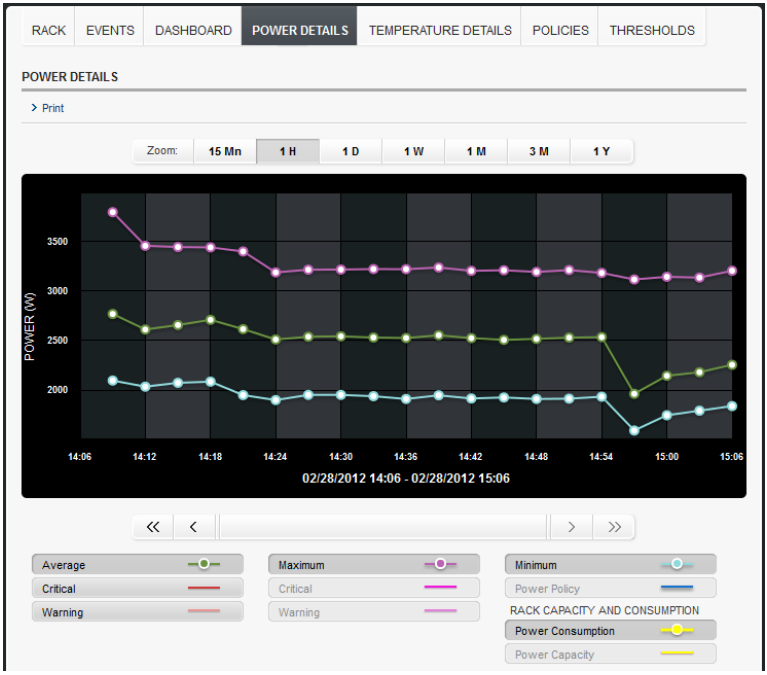
For more information on how to configure default units and energy consumption, see "Energy Consumption Settings" in the "Configuring Power Center" chapter.

Viewing Power Details

Go to **Power Overview → Physical (or Logical) Groups**, click the group/device icon, and then open the **Power Details** tab to view its power details.

The **Power Details** page displays different information for PDU and other devices/groups. Power Center does not provide power details for UPS.

For devices/groups (Excludes PDU and UPS), by default, the **Power Details** graph displays the power details for the previous hour.



You can also:

View power details for the current time window

- Click a time window tab to see the current power details.

Table 10-1. Time Window and Interval

Time Window	Description	Interval
15Min	15 minutes	1 minute
1H	1 hour	3 minutes
1D	1 day	1 hour
1W	1 week	6 hours
1M	1 month	1 day
3M	3 months	1 week
1Y	1 year	2 weeks

NOTE: The table above lists the interval when the sampling interval is at the default value (1 minute). The sampling interval change will result in the interval change of 15Min and 1H time window. If you change the sampling interval to 3 minutes, the interval of 15Min time window is 3 minutes. If you change the sampling interval to 6 minutes, the interval of 15Min time window is 3 minutes, and the interval of 1H time window is 6 minutes. For more information on how to configure the sampling interval, see "Monitoring Sampling Interval" in the "Configuring Power Center" chapter.

View power details for a different time window

- Click the arrow buttons < > to see the details for the previous/next sampling time, or click the arrow buttons << >> to see the details for the previous/next page of results for the current time window.

You can click **Average**, **Maximum**, or **Minimum** to display the selected value.

- **Average:** The average value from the previous time point to the current time point.
- **Maximum:** The maximum value from the previous time point to the current time point.
- **Minimum:** The minimum value from the previous time point to the current time point.

For example, when you view power details in the 1H (1 hour) window, the maximum value at 15:00 shows 500W and the time interval is 6 minutes, this value represents the maximum power consumption from 14:54 to 15:00 is 500W.

NOTE: It is common to see some instantaneous values exceed the Power Cap value in the **Maximum** line. Power Center monitors this value and controls it to normal power range when this happens. You only need to pay attention when the **Average** power value exceeds the Power Cap value.

NOTE: You can set the time interval (period from a time point to the next time point) in the **Settings** page. For more information on how to configure the interval, see "Monitoring Settings" in the "Configuring" chapter.

For racks, you can also click **Power Consumption** to display PDU power consumption for all rack PDUs.

You can also click **Power Policies** to change a power policy.

NOTE: The **Power Policies** button is only enabled if you have configured a power policy in the **Policies** page. For more information on how to configure a power policy, see the "Power Policies" chapter.

You can view the following power details of the PDU devices. For more information on supported PDU devices, see "System Requirements" in the "Overview" chapter.

- PDU device information: Including PDU name, model and IP address.
- PDU outlet information: Including outlet number, power(W), voltage (V), amps(A), and time of the information recorded, following this format: <YYYY-MM-DD HH:MM:SS>. The table lists the information for each outlet and the total power consumption for all outlets.

NOTE: For PDU outlet information, Power Center only supports the Dell Managed Rack PDU 6605.

Viewing Energy Consumption

The **Power Details** page provides the following energy consumption information:

- IT Equipment Energy — The total energy consumption and cost for all managed devices in the selected device/group.

NOTE: Power Center can read the power consumption of a device when it is at S0 (On) state. For devices in S4/S5 state, Power Center uses a fixed value (30W) to calculate the power consumption.

- Cooling Energy — The estimated energy consumption and cost needed to cool the selected device/group.

  *Cooling Energy = IT Equipment Energy * Cooling Multiplier*

  You can configure the cooling multiplier in the **Settings → Energy Consumption** page.

- Energy Consumed (Total) — The combined energy consumption and costs for the IT equipment and cooling energy. The calculation formula is:

  *Cost = (IT Equipment Energy T1*Cooling Multiplier) *Flat Rate T1+(IT Equipment Energy T2*Cooling Multiplier) *Flat Rate T2+°¦+(IT Equipment Energy Tn*Cooling Multiplier) *Flat Rate Tn*

NOTE: T1/T2/.../Tn is the time period (in hours) at a certain flat rate.

NOTE: By default, the Cost column displays 0. You must configure the cost rate to see the cost. The rate is a global setting, and can be set on the **Settings → Energy Consumption** page.

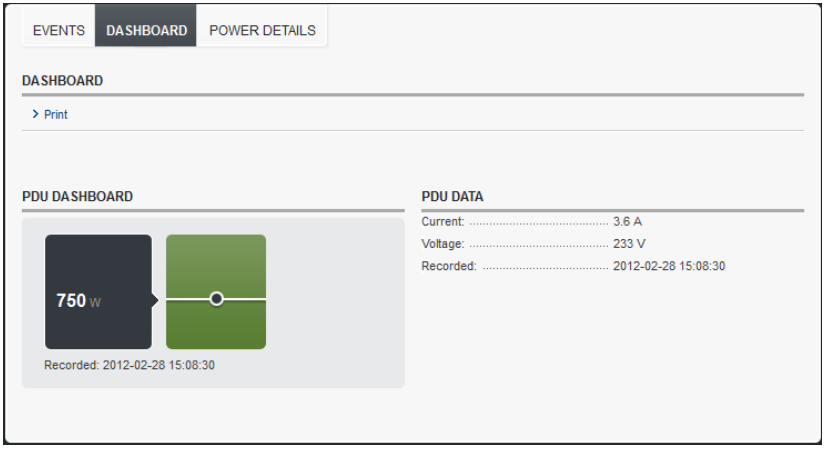
NOTE: The Energy Consumption section displays information based on the values configured in the **Settings** page. This information should be used as an estimate only.

NOTE: When a device or group is newly added or created in Power Center, the power and energy consumption data displayed in the "1W" and "1M" time windows are different if the monitored time is less than 1 week, and the data displayed in the "1H" and "1D" time windows are different if the monitored time is less than 1 day. This occurs because Power Center uses different sampling intervals for different time windows. For example, a device is added into Power Center at 2011-10-15 09:00, and the current time is 2011-10-17 11:10. For the 1M time window (sampling interval is 1 day), the power and energy consumption is calculated from 2011-09-17 00:00 to 2011-10-17 00:00. For the 1W time window (sampling time is 1 hour), the power and energy consumption is calculated from 2011-10-10 11:00 to 2011-10-17 11:00. There is a 11 hour gap therefore the data displayed in the two time windows are not the same.

Monitoring PDU Power

There are two scenarios for monitoring the PDU power:

- If you view the PDU Dashboard from the **Dashboard** page of a group: The **PDU Dashboard** displays all PDU information in a table.
- If you view the PDU Dashboard from the **Dashboard** page of a PDU: The **PDU Dashboard** displays the specific PDU information in a graph as follows:



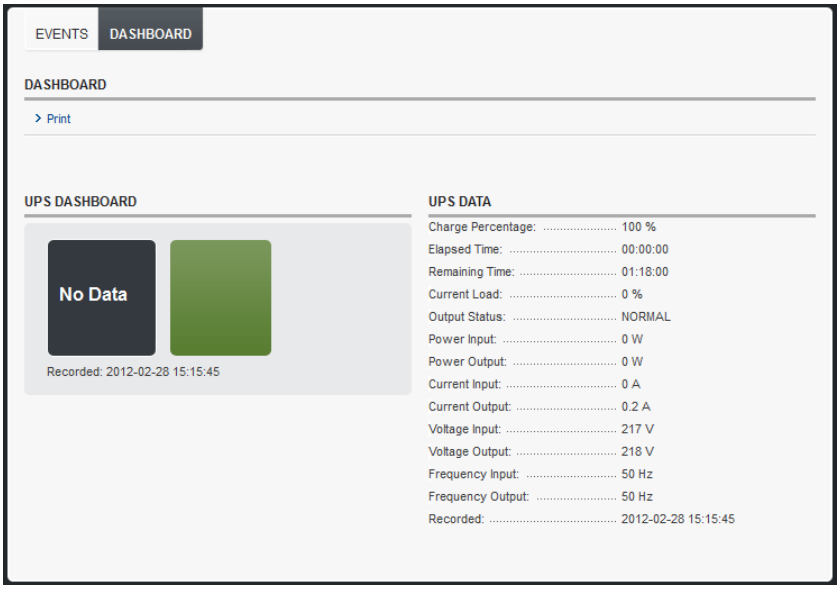
  - The left and right boxes show the instantaneous power value of the PDU.
  - The page also lists the PDU details read from the device. It displays **NA** when the data is not provided on this PDU device.

Monitoring UPS Power

There are two scenarios for monitoring the UPS power:

- If you view the UPS Dashboard from the **Dashboard** page of a group: The **UPS Dashboard** displays all UPS information in a table.

- If you view the UPS Dashboard from the **Dashboard** page of a UPS: The **UPS Dashboard** displays the specific UPS information in a graph as follows:



  - The left and right boxes show the temperature of the UPS.
  - The page also lists the UPS details read from the device. It displays **NA** when the data is not provided on this UPS device.

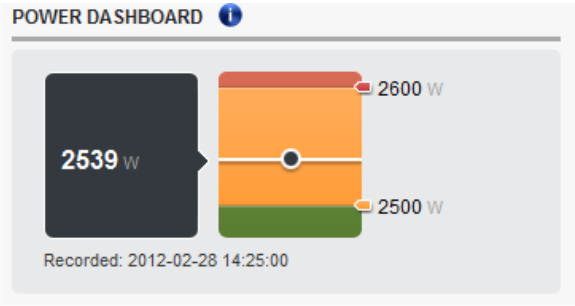
Power Dashboard

You can monitor the Power Center overall status in the **Dashboards** page.

To view the dashboard:

1. Go to **Power Overview** → **Physical/Logical Groups**.
2. Click the group/device icon, and click **Dashboards**.

The dashboard graph displays:



For devices (Excludes PDU and UPS):

- The left box displays the average power consumption of the latest sampling interval.
- The right box displays the level of this average power consumption by comparing it with the power thresholds you set in the **Thresholds** tab:

For groups:

- The left box shows the aggregated power value of the latest sampling interval for the devices with Monitor power capability in the group.
- The right box displays the level of this aggregated power value compared with the power thresholds you set in the **Thresholds** tab.

NOTE: Aggregated power value is the power value calculated by the power data aggregation. The calculation formula is case-by-case, and depends on whether the data aggregation is based on time periods or groups.

The right box displays different colors indicating different severity levels:

- Red shows the power range that triggers a critical event.
- Orange shows the power range that triggers a warning event.
- Green shows the power range that does not trigger any event.

For more information on how to configure the sampling interval, see "Monitoring Settings" in the "Configuring Power Center" chapter.

For more information on how to configure the thresholds, see "Power Monitoring Configuration" in this chapter.

Printing Power Monitoring/Dashboard Graph

Click **Print** to print the power monitoring, power dashboard graph to a PDF file or printer.

You must set the Web browser to enable the "Print Background" option and other printing settings, otherwise the results are printed either without a background or with incorrect page alignment.

To enable "Print Background" in Mozilla Firefox:

1. Go to **File** → **Page Setup** → **Format & Options**.
2. Check the option **Print Background (colors & images)**.
3. Click **OK**.

To enable "Print Background" in Microsoft Internet Explorer:

1. Go to **File** → **Page Setup**.
2. Check the option **Print Background Colors and Images**.
3. Click **OK**.

When you print the graphs in Microsoft Internet Explorer 8, you need to make sure:

- The Web browser mode is not set as Internet Explorer 7 mode.
- The following options are all selected in **File** → **Page Setup**:
  - Portrait
  - Print Background Colors and Images
  - Enable Shrink-to-Fit

11

Temperature Monitoring

Power Center enables monitoring of the current or historical temperature of the data centers in Power Center. It can help you understand the temperature status and identify hot spots in the data center.

You can monitor the temperature status at different device/group levels, you can configure the temperature monitoring settings to meet your monitoring needs, and you can print the temperature status graph.

Temperature Monitoring Level

Power Center provides temperature monitoring at the following levels:

- Device level:

  You can monitor temperature-related metrics for devices.

- Physical group level:

  You can monitor temperature-related metrics at the physical group level (data center, room, aisle, chassis modular)

- Logical group level:

  You can monitor temperature-related metrics at the logical group level.

Temperature Monitoring Configuration

You can configure temperature monitoring settings in Power Center, including:

- Thresholds (Inlet temperature range for events)
- Device and group range (Monitor all or not)
- Sampling interval (1, 3, or 6 minutes)
- Default units (Celsius or Fahrenheit)

Thresholds is useful if you want to be notified when the temperature of the group/device exceeds the thresholds. Once the temperature value exceeds a critical or warning threshold, the related event is sent.

To configure thresholds:

1. Go to **Power Overview** → **Physical** (or **Logical**) **Groups**, and click the group/device icon.
2. Go to **Thresholds** → **Temperature Thresholds**, and click **Edit**.
3. Enter values for the following:

- Critical thresholds for average inlet temperature - Greater — When the temperature is greater than the setting, the critical-level event "Average Inlet Temperature" is sent.
- Critical thresholds for average inlet temperature - Less — When the temperature is less than the setting, the critical-level event "Average Inlet Temperature" is sent.
- Warning thresholds for average inlet temperature - Greater — When the temperature is greater than the setting, the warning-level event "Average Inlet Temperature" is sent.
- Warning thresholds for average inlet temperature - Less — When the temperature is less than the setting, the warning-level event "Average Inlet Temperature" is sent.

4. Click **Apply**.

After you configured the thresholds, you will see four lines with different colors indicating the thresholds in the **Temperature Details** tab.

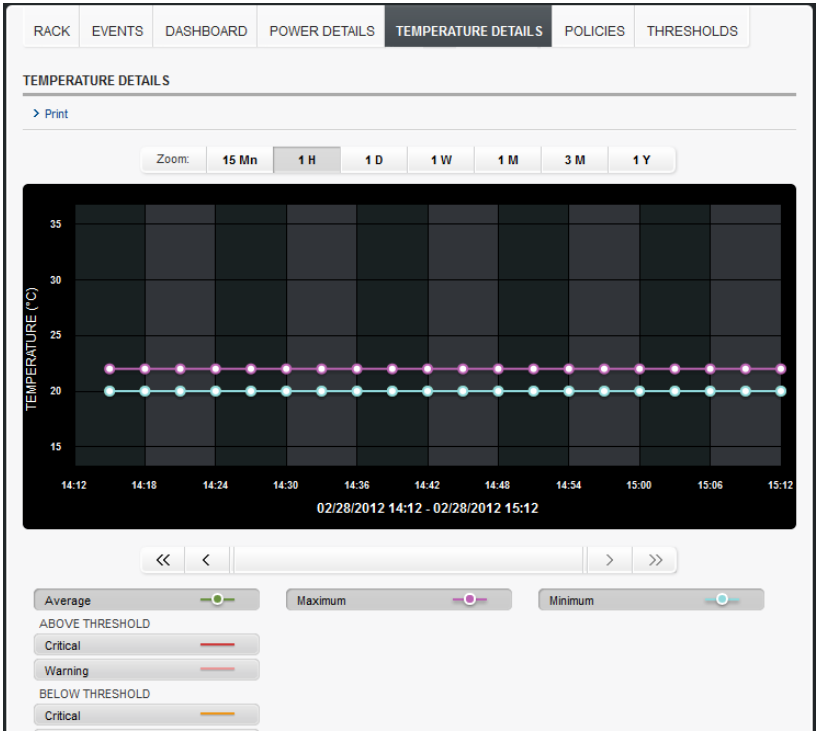
For more information on how to configure the device/group range and sampling interval, see "Monitoring Settings" in the "Configuring Power Center" chapter.

For more information on how to configure the default units and energy consumption, see "Energy Consumption Settings" in the "Configuring Power Center" chapter.

Viewing Temperature Details

Go to **Power Overview** → **Physical (or Logical) Groups** page, and click the group/device icon, then open the **Temperature Details** tab to view its temperature details.

Temperature Details:



By default, the Temperature Details graph displays temperature details of the previous hour. You can also:

- **View temperature details of current time window**

  Click a time window tab to see the current temperature details.

Table 11-1. Time Window and Time Interval

Time Window	Description	Time Interval
15Min	15 minutes	1 minute
1H	1 hour	3 minutes
1D	1 day	1 hour
1W	1 week	6 hours

Table 11-1. Time Window and Time Interval

Time Window	Description	Time Interval
1M	1 month	1 day
3M	3 months	1 week
1Y	1 year	2 weeks

NOTE: The table above lists the interval when the sampling interval is at the default value (1 minute). The sampling interval change will result in the interval change of 15Min and 1H time window. If you change the sampling interval to 3 minutes, the interval of 15Min time window is 3 minutes. If you change the sampling interval to 6 minutes, the interval of 15Min time window is 3 minutes, and the interval of 1H time window is 6 minutes. For more information on how to configure the sampling interval, see "Monitoring Sampling Interval" in the "Configuring Power Center" chapter.

- **View temperature details of a different time window**

  Click the arrow buttons **<>** to see the details of previous/next sampling time, or click the arrow buttons **<<>>** to see the details of previous/next page of results for the current time window.

You can click **Average**, **Maximum**, and **Minimum** to display the selected value.

- **Average:** The average value from the previous time point to the current time point.
- **Maximum:** The maximum value from the previous time point to the current time point.
- **Minimum:** The minimum value from the previous time point to the current time point.

For example, when you view temperature details in the 1H (1 hour) window, the maximum value at 15:00 shows 40°C and the time interval is 6 minutes, this value represents that the maximum temperature from 14:54 to 15:00 is 40°C.

Chassis Details:

The Chassis Details table appears when you access the **Temperature Details** page on a chassis. **Chassis Details** lists all blade servers within the chassis and their temperature details in a table, including:

- **Device:** Device name.

- **Average:** The average value of the latest sampling interval.
- **Maximum:** The maximum value of the latest sampling interval.
- **Minimum:** The minimum value of the latest sampling interval.

NOTE: You can set the time interval (the period from a time point to the next time point) in the **Settings** page. For more information on how to configure the interval, see "Monitoring Settings" in the "Configuring" chapter.

NOTE: The Average, Maximum or Minimum field displays **NA** if no data is available. For example, when the blade server is an Unsupported device.

Monitoring Temperature of Chassis/Blade Server

You can monitor the inlet temperature at the blade server level.

You can also monitor the inlet temperature, at the chassis level, including average, maximum, and minimum details.

Monitoring Temperature of Devices/Groups

Power Center supports temperature monitoring of the inlet temperature span for devices and groups. The inlet temperature span is the average inlet temperature differential between the maximum and minimum temperature reading for a device in a group (Celsius or Fahrenheit). You can calculate this value according to the maximum and minimum temperature from the **Temperature Details** graph.

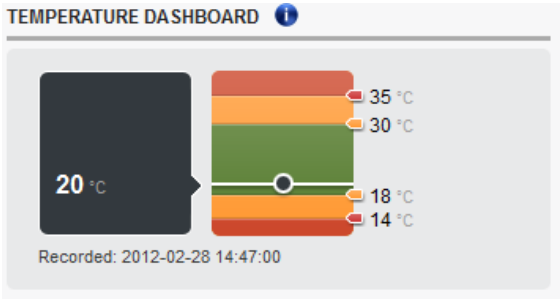
Temperature Dashboard

The **Dashboards** page displays Power Center's overall status.

To view the dashboard:

1. Go to **Power Overview** → **Physical/Logical Groups**.
2. Click the group/device icon, and click **Dashboards**.

The dashboard graph displays:



For devices (Excludes PDU and UPS):

- The left box displays the average temperature status of the latest sampling interval.
- The right box displays the level of this average temperature status by comparing it with the temperature thresholds you set in the **Thresholds** tab:

For groups:

- The left box shows the aggregated temperature value of the latest sampling interval for the devices with Monitor power capability in the group.
- The right box displays the level of this aggregated temperature value by comparing it with the temperature thresholds you set in the **Thresholds** tab.

NOTE: Aggregated temperature value is the temperature value calculated by the temperature data aggregation. The calculation formula is case-by-case, and depends on whether the data aggregation is based on time periods or groups.

The right box displays different colors indicating different severity levels:

- Red color shows the temperature range that triggers a critical event.
- Orange color shows the temperature range that triggers a warning event.
- Green color shows the temperature range that does not trigger any event.

For more information on how to configure the sampling interval, see "Monitoring Settings" in the "Configuring Power Center" chapter.

For more information on how to configure the thresholds, see "Temperature Monitoring Configuration" in the "Temperature Monitoring" chapter.

Printing Temperature Monitoring/Dashboard Graph

Click **Print** to print the temperature monitoring, and temperature dashboard graph to a PDF file or printer.

You must set the Web browser to enable the "Print Background" option and other printing settings, otherwise the results are printed either without a background or with incorrect page alignment.

For how to enable the "Print Background" option and other print settings, see "Printing Power Monitoring/Dashboard Graph" in the "Power Monitoring" chapter.

12

Power Policies

A power policy is a set of configurations used to manage the power cap for devices or groups. A policy is useful for defining power management in different situations, for example:

- You can set up a policy to make sure that the power consumption does not exceed the capacity of the circuit.
- You can set up a policy with a scheduled time according to the workload of the device/group; for example, you can set an aggressive cap when the workload is low, enabling a reduction of power use for your data center.
- You can set up a policy to increase the rack density. For example, you currently have ten devices in rack A_01 that is monitored by Power Center. By monitoring the power consumption from the **Power Details** page, you can estimate how many devices you can add to rack A_01. You can set up a policy to cap the total power consumption of rack A_01 after you added the devices.

Power Center supports two policy types:

- Static power policy — The power cap for each device is defined by you, and will not be changed unless you redefine it. A static power policy enables you to set a power cap for each device in the group. You can create a static power policy for a rack, chassis or device.
- Dynamic power policy — The power cap for each device is dynamically allocated by Power Center when necessary, based on the power consumption information and other power information on each device. Power Center evaluates power consumption for each device in every monitoring cycle to decide the necessity of changing the power cap for each device. A dynamic power policy enables you to allocate the power dynamically for each device in the group while maintaining the power cap for the group. A dynamic power policy has less performance impact to a device/group compared with a static power policy. You can create a dynamic power policy for a logical group, data center, room, aisle, rack, or chassis.

How Does a Dynamic Power Policy Work?

To understand how a dynamic policy works, you need to understand the following terms first:

- Consumption — The power a device is using.
- Power Cap — The maximum amount of power that a device is allowed to consume (may not be equal to its demand).
- Headroom — The difference between power cap and power consumption of a device or a group of devices under a power policy.
- Demand — Amount of power a device requests to accommodate its workload.

The top priority of the dynamic power policy is to maintain the power cap of the group. Maintaining this cap means that all devices can execute their workloads without needing more power than the cap. The priority of the device may not be taken into account when allocating power cap to a group of devices if most, or the entire power cap is allocated towards maintaining the power cap on each of the devices in the policy; if lower priority devices require more power to maintain their cap, they may actually receive more power than a higher-priority device. If the power cap is too restrictive and the group power consumption exceeds the power cap, an event is sent for the power policy. You need to reconsider the power allocation or adjust workloads when a power policy is consistently violated by one or more devices exceeding their power cap.

If fluctuations in device power requirements happen once the power cap is successfully established for all devices in a power policy, a device requiring more power may not get it as the power cap of another device in the policy could become violated as it is lowered. If you wish to force one or more devices in a policy to a lower cap, you can create a static power policy for the device at a lower level. In this case, the most restrictive power cap of the overlapping policies is applied to the device.

If there is excess available power from the power cap (known as *headroom*) after the power capping requirements is met for all devices in the policy, then this excess power can be allocated dynamically according to the priority and demand of the device in the power policy.

If the average power consumption of a device becomes lower than the power cap established for the device, its power cap is evaluated and adjusted in each monitoring cycle, and the excess power is deemed as headroom for other devices to consume.

Power Policy Capabilities

Power Center defines the following statuses of power policy capabilities for the devices:

- Unknown — Shown for unsupported devices or devices that were never connected to Power Center.
- None — No power policy capability. You cannot set any policy on the device.
- Monitor — With power monitoring capability only.
- Monitor & Capping — With power monitoring and capping capabilities.
- Monitor and Upgradable — With power monitoring capability, and can be upgraded to have power capping capability.

You can find this power policy capability status in the **Power Capability** column of the **Device List** page.

For servers that comply with Dell iDRAC7, when there is a power policy capability change due to a license change, Power Center will change its information in the management console within 24 hours. There are two scenarios:

Scenario 1. The license expires or is not imported

In this case, the following happens:

- If a policy exists on the devices, you will receive a "Server Capabilities Changed" event.
- The **Policy** tab of the devices is set to disabled in the **Power Overview** page.
- The power capability status of the devices is set to "None" in the **Device List** page.
- You cannot edit the policy of this device from the **Policies** page; you only can delete it.

Scenario 2. You try to import a license on a device without a license imported

In this case, the following happens:

- If a policy exists on the devices, you will receive a "Server Capabilities Changed" event.
- The **Policy** tab of the devices is set to **Enabled** in the **Power Overview** page.
- The power capability status of the devices is changed in the **Device List** page.
- The policy of the devices is editable. You can access it from the **Policies** page.

Upgrading Device Power Policy Capability

The power policy capability of some devices can be upgraded to include capping of power consumption, for example, Dell PowerEdge M620. These devices show **Monitor and Upgradable**. To upgrade the device so that its power consumption can be capped, go to the **Device List** page and click **Upgrade** next to the device, then follow the instructions on the pop-up help page to upgrade the device power capability. Once the upgrade is completed, the power capability status changes to **Monitor & Capping** within 24 hours.

Creating a Policy

You can create static or dynamic policies for your device/group.

You can create static power policies for a rack, chassis or device, and create dynamic power policies for any group/device. Power policies only apply to the groups/devices that have Monitor & Capping power capability.

You can create multiple policies on the same device/group. This is useful when you want to apply different policies at different time periods for the same device/group.

To create a new policy:

1. Go to **Power Overview** → **Physical/Logical Groups** page.
2. Click the rack/chassis/device icon, and go to the **Policies** tab.
3. Click **Create New Policy**.

4 The **Create New Policy** window opens, set a power cap using the following steps:

a Enter a policy name, maximum length of no more than 25 English characters.

b Select **Static** or **Dynamic** from the **Policy Type** drop-down list. This step is available only when you create a policy on a rack/chassis.

c Select a fixed time period to show **Average Power** and **Maximum Power** values to estimate a Power Cap value. The **Average Power, Maximum Power**, **Lower Bound** and **Upper Bound** values only refer to the devices that have Monitor & Capping power capability.

d Enter **Power Cap Value** or **Percentage of Capability** for the group/device:

- **Power cap value:** Enter a value between the **Lower Bound** and **Upper Bound**. The Lower Bound is the lowest minimum power consumption since the device/group was either discovered/added. The Upper Bound is the maximum power consumption when the device/group is in a maximum workload state. You cannot enter a power cap value lower than the Lower Bound value. This value is the total power consumption budget for devices that have Monitor & Capping power capability.
- **Percentage of capability:** Enter a percentage (1%-100%) of the Upper Bound value to set the power cap.

The "Power Cap Value" and "Percentage of Capability" are related values. The following formula describes the relationship between the two values:

*Upper Bound * Percentage of Capability = Power Cap Value*

e Click **Next**.

NOTE: The default power cap unit is Watts. You can change this to a different unit. For more information on how to change the default unit, see "Default Units Settings" in the "Configuring Power Center" chapter.

5 Allocate power for the group/device:

- For a dynamic policy, the priority (High, Medium, and Low) for the individual devices in the group can be changed as needed. After selecting the priority, click **Next**.

NOTE: All devices are displayed on this page, but you only can configure priority for the devices that have Monitor & Capping power capability.

NOTE: You can set priority levels based on the service level agreements associated with workloads running on different devices/groups. Power Center reserves more of the power for the devices/groups with a higher priority when the power cap is not completely utilized.

- For a static policy, Power Center uses the same percentage of the Upper Bound value as the power cap for each device by default. You can enter a different value (Power Cap Value or Percentage of Capability), and click **Next**.

NOTE: If the sum of the entered device power cap is higher than the power cap value set in the previous step, Power Center will change the Power Cap Value and display a message prompt.

6 Enter a policy schedule that includes:

- Time Stamp — Time of the day.
  - Always — The policy is in effect all the time.
  - Range — Enter the start time and end time of the day for the policy to take effect. You can enter any time between 00:00 and 23:59. If you have entered a start time that is later than the end time, for example, 23:00 – 07:00, the effective timespan will be 23:00 of the current day to 07:00 of the next day.
- Recurrence Pattern — Day of the week.
  - Always — The policy is in effect from Monday to Sunday.
  - Day of the week — Select the days of the week for the policy to take effect.
- Recurrence Range —Start and end dates.
  - Always — The policy is in effect all year round.
  - Range — Enter the start and end dates for the policy to take effect.

After you have defined the schedule, click **Next**.

7 Review the policy summary information, and click **Apply**. The new policy is created and takes effect immediately.

NOTE: The existing power cap value set in the policies (including EPR) still remain effective on the devices even if Power Center is corrupted; this impacts the performance of the devices with policies applied. You must back up Power Center

data on a regular basis to avoid such impacts. To restore the policies after Power Center is corrupted, perform the following steps: 1) Reinstall Power Center. 2) Use the backup data to recover. After completing the two steps, you can use the previously-existing policies to control the devices. For more information on Power Center data backup and recovery, see the "Backup and Recovery" chapter.

Viewing Policy Details

You can view policies from the following pages:

- **Policy** page — This page lists all policies. You cannot create a policy on this page. You can edit, delete, sort, filter or enable/disable the policies.
- **Power Overview** → **Policy** page — This page lists policies for a specific entity. To view the policies, go to the **Power Overview** page, select a physical group or logical group, select an entity and click its **Policies** tab. You can create, edit, delete, sort, or enable/disable the policies on this page.

These two pages display policy details:

- Enabled — The policy is enabled or disabled.
- Active — The policy is in use or not in use.
- Entity Name — Name of the entity.
- Policy Name — Name of the policy.
- Type — Static power policy or dynamic power policy.
- Power Cap — Power cap for the entity.
- Date Range — Start date and end date for the policy to take effect.
- Time Range — Time of the day for the policy to take effect.
- Days — Day of the week for the policy to take effect.

Policy Priority Levels

When you create or update a policy, you can select different priority levels for each device/group. For example, you can set priority levels based on the service level agreements associated with workloads running on a device/group.

Power Center tends to reserve more power to the devices/groups with higher priority when the power cap for devices/groups is not fully utilized.

For each device/group, you can set one of the three priority levels:

- Low
- Medium (Default)
- High

Priority lists are policy-specific; however a device/group may have different priority levels in different policies. A higher-priority value of a device/group in a policy overrides the lower-priority value of the same node in another policy.

For example, you created Policy1 for device <A, B, C> and Policy2 for device <B, C, D>, and you configured different priorities or power caps for the policy with the same time slot. In this case, Power Center follows these rules:

- If there are overlapping policies on an entity, the policy with the lowest power cap is applied.
- If there are overlapping dynamic policies on an entity and both are currently active, the highest priority (High > Medium > Low) of this entity is applied.

Policy Modes

The policy mode is shown in the Enabled and Active columns in the **Policies** page. A green symbol indicates Enabled or Active. Power Center supports three policy modes:

Table 12-1. Policy Modes

Enabled Column	Active Column	Mode	Description
Green	Green	Enabled and active	The policy is in use now.
Green	NA	Enabled but not active	The policy is available but not in use now.
NA	NA	Disabled	The policy is created but not available for use.

Enabling/Disabling Policy

After you create a new policy, it is enabled by default.

To disable or re-enable a policy:

1. Go to the **Policies** page or the **Policies** tab in the **Power Overview** page.
2. Click **Enable/Disable**.
3. Check or uncheck the **Enabled** box for the policy.
4. Click **Apply**.

Displaying Policies in the Power Details Graph

You can view the policies in the **Power Details** graph.

To display a policy:

1. Go to **Power Overview** → **Physical/Logical Groups**.
2. Click the icon of the device/group, and go to the **Power Details** tab.
3. Click **Power Policy** under the graph.
4. Click **Select Power Policy**, and select a policy.

The policy implementation status is displayed in the **Power Details** graph.

To hide a policy:

Click **Power Policy** again.

Updating a Policy

To update a policy:

1. Go to the **Policies** page or the **Policies** tab in the **Power Overview** page.
2. Click **Edit** next to the selected policy.
3. The **Edit Policy** window opens. Update the policy details. See "Creating a Policy" in this chapter.
4. Click **Apply**. The policy is updated and takes effect immediately.

Deleting Policies

To delete policies:

1. Go to the **Policies** page or the **Policies** tab in the **Power Overview** page.
2. Click **Delete**.
3. Select the policies' checkboxes to delete them.

4 Click **Apply**.

Filtering Policies

You can apply a filter to show only specific policies.

To filter policies:

1 Go to the **Policies** page.

2 Click **Filter**.

3 The **Filter** window opens. Click a filtering option in the left pane - **Policy Type**, **Power Cap**, or **Policy Status** - to display a specific filtering option window.

4 In the filtering option window, use the displayed information to select the filtering options. You can use one or more options to filter policies.

- **Policy Type** — Select the static power policy or dynamic power policy. You can select multiple policy types.
- **Power Cap** — Define the power cap range for the device/group by setting the minimum and maximum power cap values.
- **Policy Status** — Select the status of the policy. The status can be Enabled, Disabled and Active, Inactive. You can select multiple options.

5 Click **Apply**. The **Policies** page displays the filtered policies.

Emergency Power Reduction

When there is an emergency situation, for example, if there is a power failure and the devices are running on the UPS, you can initiate Emergency Power Reduction to set the power consumption to minimal.

WARNING: Applying emergency power reduction will throttle power on the devices down to an extremely low level, which will impact performance. All the devices with Monitor & Capping power capability are impacted. Use this only in an emergency situation.

To initiate an emergency power reduction:

1 Go to **Power Overview** → **Physical/Logical Groups**.

2 Click the icon of the device/group, and go to the **Policies** tab.

3 Click **Emergency Power Reduction** in the upper-right corner.

4 In the **Emergency Power Reduction** window, read the message, and click **Continue**.

All of the devices with the Monitor & Capping power capability within this group are set to the minimal power consumption state. The **Emergency Power Reduction** button appears in the upper-right corner of all pages. The devices impacted by emergency power reduction are marked with **In EPR** in the **Power Overview** and **Group Management** pages.

To cancel emergency power reductions:

1 In the upper-right corner of any page, click **Emergency Power Reduction**. The **Emergency Power Reductions** window opens.

2 In the **Remove** column, select the devices/groups from which you want to cancel emergency power reduction. You can select multiple devices/groups.

3 Click **Apply**. The **In EPR** text of the device/group disappears in the **Power Overview** and **Group Management** pages. The **Emergency Power Reduction** button disappears when you have removed all devices/groups from the **Emergency Power Reductions** window.

Policy-Related Events

When a device/group that is configured with a policy has a group structure change, for example, a device or group is deleted, moved, or added, a Warning event is sent. For more information on policy-related events, see "Pre-defined Events" in the "Event Management" chapter.

13

Comparing

Power Center enables you to add a device or a group to compare their power and temperature status and energy consumption in the selected time period. For example, you can select two rooms to compare the temperature, or select two groups with similar devices to compare their power consumption, or you can compare the data from one group in two different time periods. You can also print the comparison results.

The power and temperature information that you can compare includes:

- Power consumption — Average, maximum, minimum and peak time power consumption.
- Temperature — Average, maximum and minimum temperature.
- Energy — Total energy consumption and cost, including IT energy and cooling energy.

To compare the groups/devices, go to the **Compare** page and complete the following two steps:

1. Change the Time Period.
2. Add a Device or Group.

Changing the Time Period

You can select a date and time range to compare the monitored power and temperature status of the devices within the selected period.

To select a date and time period:

1. Click **Change Time Period**.
2. Select start date and end dates from **Date From** and **Date To**. You can either select from the calendar, or manually enter the dates following this format: <YYYY-MM-DD>.
3. Select start and end times from **Time From** and **Time To**. You can select from the drop-down list. If you need to compare the data for one day (24 hours), select 00:00 of this date and 00:00 of the next day to compare.
4. Click **Apply**.

Adding a Device or Group

You can add one to three devices or groups to compare the power and temperature status. Only one device or group can be added at a time.

To add a device or group:

1. Click **Add Device or Group**.
2. Click a category in the left pane - **Physical Group**, **Logical Group**, or **All Devices** - to display a specific group/device selection window.
3. In the selection window, use the displayed information to select a group or device.

- **Physical Group:**
  - a. The group selection window lists the physical groups as active links. Click an active link to expand the group to display all groups that are part of that physical group.
  - b. Click a physical group's active link, and then click **Select**.
  - c. The physical group is added to, and displayed in, the **Compare** page.
- **Logical Group:**
  - a. The group selection window lists the logical groups as active links.
  - b. Click a logical group's active link.
  - c. The logical group is added to, and displayed in, the **Compare** page.
- **All Devices:**
  - a. The group selection window displays a list of all devices.
  - b. Click **Select** to add the device to the **Compare** page.

4. Return to the **Compare** page to perform a comparison.

Removing/Changing Device or Group

To remove a group or device from comparison, click the X button of the selected device/group.

To change a device/group for comparison, remove the device/group first, then add a different device/group.

Printing the Comparison Result

To print the comparison result, click **Print** on the **Compare** page.

You must set the Web browser to enable the "Print Background" option and other printing settings, otherwise the results are printed either without a background or with incorrect page alignment.

For how to enable the "Print Background" option and other print settings, see "Printing Power Monitoring/Dashboard Graph" in the "Power Monitoring" chapter.

14

Event Management

This chapter provides information on event types, severity levels, supported PDU/UPS events, and how to manage the events in Power Center.

You can receive events indicating an abnormal power/temperature situation in the data center.

Power Center detects these types of events:

- Pre-defined events
- Custom events

The internal event listening port of Power Center is 6553; Power Center uses this port to receive events from Power Center internal. If an application uses port 6553, make sure to change it and reserve this port for Power Center.

The default external event listening port is 162; Power Center uses this port to receive events from the external devices. If the SNMP Trap service exists and uses port 162, Power Center automatically uses port 1162 to receive the external events forwarded by the SNMP Trap service.

Pre-defined Events

A pre-defined event is an event that Power Center defines based on system conditions. Power Center defines the following events (A-Z) at different severity levels.

Table 14-1. Pre-defined Events

Type	Description	Severity Level
Blades Change In Chassis	Some blades in a chassis are changed; you must manually re-discover the chassis. **NOTE:** Power Center detects the chassis change once every 15 minutes.	Informative
Cannot Register Event on Device	The device cannot register the device events to the Power Center server automatically.	Warning

Table 14-1. Pre-defined Events

Type	Description	Severity Level
Communication with Chassis Failed	Power Center lost communication with the chassis.	Warning
Communication with Chassis Restored	Power Center restored communication with the chassis.	Informative
Communication With Node Failed	Power Center lost communication with the device.	Warning
Communication With Node Restored	Power Center restored communication with the device.	Informative
Database Maintenance Success	The database maintenance completed successfully.	Informative
Hierarchy Change Policy	A group structure has affected a policy.	Warning
Internal Error	Power Center internal error.	Warning
IPMI Power Unit	Events related to the server power unit.	Critical
IPMI Power Supply	Events related to the server power supply.	Critical
IPMI Processor Temperature Trip	Events related to the server processor temperature trip.	Critical
IPMI Fan	Events related to the server fan.	Critical
IPMI Test	An IPMI test event was received.	Informative
Kerberos SSO Initialization Failed	SSO initialization failed because Kerberos-related configuration is incorrect.	Warning
UPS Bad Battery	Events related to battery failure in the UPS.	Critical
UPS Low Battery	Events related to low battery limits and exceeded thresholds in the UPS.	Critical

Table 14-1. Pre-defined Events

Type	Description	Severity Level
UPS Bad Temperature	Events related to temperature limits and exceeded thresholds in the UPS.	Critical
UPS Bad Input	Events related to power input failure in the UPS.	Critical
UPS Bad Output	Events related to power output failure in the UPS.	Critical
UPS Overload	Events related to output power load limits and exceeded thresholds in the UPS.	Critical
UPS On Bypass	Events related to on bypass in the UPS.	Informative
UPS Bad Bypass	Events related to bypass failure in the UPS.	Critical
UPS Shutdown	Events related to UPS shutdown.	Informative
UPS Charge Failure	Events related to charge failure in the UPS.	Critical
UPS Fan Failure	Events related to power fan failure in the UPS.	Critical
UPS Communication Lost	Events related to communication lost in the UPS.	Warning
Protocol Timeout Change Failed	Protocol timeout change has failed.	Warning
PDU High Load	The PDU power is greater than the high load threshold.	Warning
PDU Low Load	The PDU power is lower than the low load threshold.	Warning
PDU Overload	The PDU is overloaded.	Critical
PDU Outlet High Load	The PDU outlet power is greater than the high load threshold.	Warning
PDU Outlet Low Load	The PDU outlet power is lower than the low load threshold.	Warning
PDU Outlet Overload	The PDU outlet is overloaded.	Critical

Table 14-1. Pre-defined Events

Type	Description	Severity Level
PDU Outlet Off	The PDU outlet is Off.	Informative
PDU Outlet On	The PDU outlet is On.	Informative
Server Capabilities Changed	The server capabilities have changed, for example, a license change. **NOTE:** The "Server Capabilities Changed" event is only applicable to a device that has a policy applied. When you see such an event, check the policy on the device.	Warning

NOTE: To receive events from a PDU or UPS, you must subscribe to the event from the console of that PDU/UPS.

NOTE: For the Power Center supported IPMI events (IPMI Power Unit, IPMI Power Supply, IPMI Processor Temperature Trip, IPMI Fan), Dell PowerEdge tower servers and rack servers support all these IPMI events, and Dell PowerEdge blade servers only support IPMI Processor Temperature Trip events.

NOTE: Power Center only supports IPMI trap format for Dell iDRAC devices. To receive events from a Dell iDRAC device, make sure the alert function is enabled and the IPMI trap format is selected for all the Power Center-supported events (IPMI Power Unit, IPMI Power Supply, IPMI Processor Temperature Trip, IPMI Fan) in the iDRAC management console. For example, in the Dell iDRAC7 management console, you must select IPMI trap for all PWR/PSU/CPU/Fan-related alerts. For more information on how to use the Dell iDRAC management console, see Dell iDRAC Help.

Custom Events

A custom event is triggered when the custom condition threshold is reached.

Power Center provides the following custom events:

Table 14-2. Custom Events

Type	Description	Severity Level
Average Power	Average power consumption is greater than the average value you set in the Thresholds.	Critical or Warning; depends on the threshold type

Table 14-2. Custom Events

Type	Description	Severity Level
Average Inlet Temperature	Average temperature is greater or less than the average value you set in the Thresholds.	Critical or Warning; depends on the threshold type
Max Power	Power consumption is greater than the maximum value you set in the Thresholds.	Critical or Warning; depends on the threshold type
Policy Cannot Be Maintained	Policy cannot be maintained because the average power consumption of the devices with power capping capability that relate to this policy, exceed the power cap value of this policy.	Critical
Policy Return To Normal	Policy can be maintained now because the power consumption is less than the power cap value.	Informative
Power Return To Normal	Power consumption returned to the normal range you set in the Thresholds.	Informative
Temperature Return To Normal	Temperature returned to the normal range you set in the Thresholds.	Informative

When the following change occurs, the corresponding "Critical" or "Warning" event becomes an "Informative" event:

- "Power/Temperature Return to Normal" event is triggered.

  For example, for Average Inlet Temperature, if you set 50 °C as the Critical threshold and 40 °C as the Warning threshold, when the average temperature reaches 60 °C, Critical and Warning events are sent. When the average temperature returns to 45 °C, the Critical event automatically becomes Informative. When the average temperature returns to 35 °C, the "Warning" event automatically becomes "Informative".

When the following change occurs, the corresponding "Critical" event becomes an "Informative" event:

- A device/group is removed from Power Center.

- An event condition is removed from Power Center, for example, the Threshold settings.
- An event condition is updated in Power Center, for example, the Threshold settings.
- A power policy is removed or disabled.
- "Policy Return To Normal" event is triggered.

For more information on the thresholds, see "Power Monitoring Configuration" in the "Power Monitoring" chapter and "Temperature Monitoring Configuration" in the "Temperature Monitoring" chapter.

Supported PDU/UPS Events

Power Center supports different events for different PDU and UPS. The following table lists the events that were validated by Power Center. There may be other events.

Table 14-3. Supported PDU/UPS Events

PDU/UPS Model	Supported Events
Dell UPS	UPS Low Battery, UPS Bad Input
APC UPS	UPS Low Battery, UPS Shutdown, UPS On Bypass
Eaton UPS	UPS Low Battery, UPS Bad Input, UPS Bad Battery
Emerson UPS	UPS Low Battery
Dell PDU	PDU Low Load, PDU High Load, PDU Overload, PDU Outlet Low Load*, PDU Outlet High Load*, PDU Outlet Overload*, PDU Outlet On*, PDU Outlet Off* **NOTE:** Events marked with * are only supported on Dell Managed Rack PDU 6605.
APC PDU	PDU Low Load, PDU High Load, PDU Overload
ServerTech PDU	PDU High Load, PDU Outlet On, PDU_Outlet Off
Emerson PDU	PDU Low Load, PDU High Load, PDU Overload

Event Severity Levels

The following table lists the severity levels for Power Center events:

Table 14-4. Event Severity Levels

Severity Level	Icon	Description
Critical		For errors that caused the managed devices or Power Center to stop working properly. You need to take action to solve the issue.
Warning		For errors that require attention. You need to look into the root cause and decide whether to take action.
Informative		An indication of an event that is not an error or warning. This is an informational event; you do not need to take any action.

NOTE: There may be an inconsistency between the severity levels defined in Power Center and the levels defined on monitored devices. For example, a severe-level event in other platforms might be a warning-level event in Power Center.

Viewing Events

You can see the critical events notification from the **Current Status** section in the left pane of the Power Center management console, with the total critical events number shown.

You can view events from the following pages:

- **Power Overview page**

This page lists events at Critical and Warning severity levels only.

Go to **Power Overview → Physical/Logical Groups**. This page displays events at different device/group levels. The events you see at a device/group level include all the events that occurred on the groups/devices within this device/group.

This page lists events for critical and warning severity levels, from most recent to earlier. You can click the arrow buttons < > to see the previous/next page.

- **Event Logs page**

This page lists all the events at all severity levels.

Go to the **Event Logs** page. You can click the arrow buttons <> to see the previous/next page.

Sorting Events

In the **Event Logs** page, by default, the events are listed by **Timestamp** in descending order (from most recent to earlier). To sort by a field, click the Up or Down symbol next to the field to list events in ascending or descending order. The symbol of the current sorted field is displayed in orange.

Editing Events

When you want to edit an event, for example, you want to put a note to describe why this event was triggered or the action that was taken, you can add a comment to the event.

To add a comment to an event:

1. Go to the **Event Logs** page.
2. Click the icon in the **Comments** column.

Table 14-5. Event comments icon and description

Icon	Description
	There is an existing comment. You can click to add more comments.
	There is no comment. You can click to add a comment

3. The **Event Comment** window opens. Click **Add Comment**.
4. Enter your comment in the **Descriptions** field, and click **Apply.**

NOTE: The maximum length for a comment is 512 characters.

NOTE: The comment cannot be edited after you click **Apply**. You can only add more comments. Power Center automatically adds the **User Name** and **Time Stamp** information to each comment.

Deleting Events

Power Center automatically deletes old events according to your database purge settings. For more information on database purge settings, see "Database Policy Settings" in the "Configuring Power Center" chapter.

You can also manually delete events in Power Center.

To delete events:

1. Go to the **Event Logs** page.
2. Click **Delete** → **Delete**.
3. Select the events' checkboxes to delete them., and click **Apply**.

To delete all events:

1. Go to the **Event Logs** page.
2. Click **Delete** → **Delete All**.
3. A message window appears; read the message and click **Yes**. All the events currently listed on the page will be deleted.

Filtering Events

If many events occurred and you want to view specific events, for example, critical events of last week, you can filter the events.

To filter events:

1. Go to the **Event Logs** page.
2. Click **Filter**.
3. The Filter window opens. Click a filtering option in the left pane - **Date Range**, **Severity**, or **Type** - to display a specific filtering option window.
4. In the filtering option window, use the displayed information to select filtering options. You can select multiple filtering options.

- **Date Range** — Enter the event start and end date. You can either manually enter the dates following this format <YYYY-MM-DD>, or select the dates from the calendar. Only events from 00:00:00 of start date to 00:00:00 of the next day after the end date are displayed. For example, you entered the filtering option 2012-01-01 as both start date and end date; all events from 00:00:00 of 2012-01-01 to 00:00:00 of 2012-01-02 are displayed.
- **Severity** — Select the event severity level. You can select multiple severity levels.

- **Type** — Select the event type. You can select multiple event types. Only the Maximum Power, Average Power, Average Inlet Temperature and the event types that currently exist in the **Event Logs** page are available for selection.

5 Click **Apply**. The **Event Logs** page displays the filtered events.

Filtering Events by Group/Device

You can filter the events by a group or device.

To filter events by a group or device:

1 Click a filtering option in the left pane - **Physical Group**, **Logical Group**, or **All Devices** - to display a specific filtering option window.

2 In the filtering option window, use the displayed information to select the filtering options. You can select one group or device.

- **Physical Group:**
  - a The filtering option window lists the physical groups as active links. Click the active link to expand the groups to display all groups that are part of that physical group.
  - b Click a physical group's active link, and then click **Select**.
- **Logical Group:**
  - a The filtering option window lists the logical groups as an active link.
  - b Click a logical group's active link.
- All Devices:
  - a The filtering option window displays a list of all devices.
  - b Click **Select** next to a device.

3 The **Event Logs** page displays the filtered events.

Sending Test Events from an IPMI Device

Power Center enables you to view test events sent from an IPMI device, therefore, you can verify the event channel between the IPMI device and Power Center server.

Before sending a test event, make sure:

- The IPMI device is added in the **Device List** page.
- The network connection status of the IPMI device is "connected."
- The Power Center server address is added in the event destination list of the IPMI device.

To send a test event from an IPMI device, see the following example for Dell PowerEdge M610:

1. Access the iDRAC management console of Dell PowerEdge M610, and go to the page related to the SNMP trap setting.
2. Click **Send** next to the Power Center server address to send a test event.
3. Access the Power Center management console. You can see that the informative event "IPMI Test" appears in the **Event Logs** page.

For more information on step 1 and 2, see the IPMI device Help.

15

Security

Power Center is designed to ensure data confidentiality, data integrity and the security of user authentication. Power Center not only provides authentication and access control to user accounts (see the "Access Conrol" chapter), but also protects all the communication channels to the Power Center server, and the stored sensitive data (for example, passwords) on Power Center server.

See the following guideline and facilities to enhance the security for your Power Cener system:

- Starting services with a normal Windows operating system (OS) user account: After installing Power Center, the Power Center services are logged on with the Network Service account by default. You can use a normal Windows OS user account instead of the Network Service account. The Windows OS user account provides better security.
- OS hardening: You can deploy OS hardening on the OS where Power Center is installed. By doing so, the minimum security foundation is set up for Power Center security-related configurations.
- Audit log: Power Center tracks the action log for critical user operations, including user login/logout, emergency power reduction, start/stop network discovery, security configuration and policy change.
- Certificate management: Power Center enables SSL/TLS communication between the Power Center management console and the Power Center server, and the communication between the Power Center server and chassis, to enforce the confidentiality and data integrity of the communication. The SSL/TLS authentication is certificate-based. Power Center uses a keystore file to manage the certificates.

Starting Services with a Normal Windows OS User Account

To configure a normal Windows OS user account, follow these steps:

1 Stop all Power Center services.

1. Go to **Control Panels → User Accounts**, and create a new normal user (either local or domain), or select an existing normal user. For example, user A.
2. Grant **Full Control** permission of the following directories or files to user A.

   Directory:

   - Dell\OpenManagePowerCenter\bin
   - Dell\OpenManagePowerCenter\external\apache-tomcat
   - Dell\OpenManagePowerCenter\external\pgsql\bin
   - Dell\OpenManagePowerCenter\logs
   - Dell\OpenManagePowerCenter\pgdata

   File:

   - Dell\OpenManagePowerCenter\conf\user.config.xml
   - Dell\OpenManagePowerCenter\conf\app.config.xml
   - Dell\OpenManagePowerCenter\external\apache-tomcat\conf\context.xml
   - Dell\OpenManagePowerCenter\external\apache-tomcat\conf\server.xml
   - Dell\OpenManagePowerCenter\external\apache-tomcat\conf\tomcat-users.xml
   - Dell\OpenManagePowerCenter\external\apache-tomcat\conf\web.xml
   - Dell\OpenManagePowerCenter\external\jre\lib\security\krb5.conf
   - Dell\OpenManagePowerCenter\external\jre\lib\security\login.conf
   - Dell\OpenManagePowerCenter\keystore.ssl
   - Dell\OpenManagePowerCenter\pgdata\pg_hba.conf
   - Dell\OpenManagePowerCenter\pgdata\postgresql.conf
3. Delete all content under **Dell\OpenManagePowerCenter\external\apache-tomcat\work**.
4. Update the Properties of the Power Center services to use normal user A to log onto service. When system notifies "The account .\A has been granted the Log On As A Service right", press **OK** to confirm.

5 Start all Power Center services to take effect.

OS Hardening

To deploy Power Center security hardening configuration on an OS where you intend to install Power Center, you must configure the basic OS hardening settings as follows:

- Installation Settings
  - Do not install Power Center and its database in the system volume.
  - Do not install Power Center and its database in the domain controller.
- Service Pack and Hotfix Settings
  - Install all critical or important service packs and hot fixes.
  - For Windows 2003, use version SP2 or above.
- Account Policy Settings

  For Windows 2003, Windows 2008 and Windows 7/Vista:
  - Use minimum password length.
  - Use maximum password age.

  For Windows 2008 and Windows 7/Vista:
  - Apply all the account policies in the Center for Internet Security (CIS) 2008 and Windows 7/Vista hardening benchmark.
- User Rights Settings
  - Apply all the user rights hardening requirements for Windows 2003, Windows 2008 and Windows 7/Vista of CIS benchmark.
- Security Options Settings
  - Apply all the security option hardening requirements for Windows 2003, Windows 2008 and Windows 7/Vista of CIS benchmark; includes the requirements for domain controller.
- File and Registry Permission Settings
  - Apply the hardening requirements for Windows 2003 of CIS benchmark.

For more information on CIS benchmark, see **http://cisecurity.org**.

For more information on Power Center supported OS, see "System Requirements" in the "Overview" chapter.

Audit Log

Power Center tracks critical operations and stores related information in a log file for auditing purposes.

Each log includes the following basic information:

- User name
- Time
- Action
- Details: Depends on the action; see the following table.

The tracked **Details** include:

Table 15-1. Audit Log Details

Action	Tracked Information
Successful/failed user login/logout	Source IP
Add/remove emergency power reduction	Impacted single device/group
Set/update/remove power policy	Impacted single device/group
Start/stop network discovery	Network discovery information; includes protocol profile, IP range.
Change session timeout	Old/new value of timeout
Change password for Power Center managed user	User name
Update role privilege	Role name, old/new value of privileges
Add/remove user to role	User name, old/new value of role name
Add/remove user	User name

The event logs are kept in the log file. You can find the log file(s) in:
<*InstallDir*>OpenManagePowerCenter\logs\Audit.log.x

The total size of all audit log files is limited to 20MB; they are evenly split into three log files (approximately 6.67MB each). If a new log causes the file size to exceed the limitation for a single log file, Power Center renames the log file to a new name, and stores the new log in a new log file with the original file name.

When generating an audit log file, the naming rule is as follows:

- audit.log — The first audit log file name. This file always logs the latest actions.
- audit.log.1 — The second audit log file name. This is copied from *audit.log* when it exceeds the file size limitation.
- audit.log.2 — The third audit log file name. This is copied from *audit.log.1* when audit.log exceeds the file size limitation.

Power Center keeps up to three audit log files. When the three files exist and *audit.log* exceeds the file size limitation, *audit.log.1* overwrites *audit.log.2*, and *audit.log* overwrites *audit.log.1*.

Managing Certificates

Power Center uses Keytool to generate a key pair (a public key and an associated private key); it wraps the public key into a self-signed certificate during the installation.

Keytool is a key and certificate management utility from Java Runtime Environment, it is located at <*InstallDir*>\external\jre\bin\keytool.exe. The private key and the self-signed certificate are stored in the keystore file at <*InstallDir*>\keystore.ssl. The self-signed certificate expires three months after installation. It is strongly recommended to update the private key and self-signed certificate within three months.

You can manage Power Center certificates through the Keytool. Possible common scenarios include:

- Scenario 1 — Generate a key pair and self-signed certificate

  During the installation of Power Center, a key pair and self-signed certificate are generated for the Power Center server.

NOTE: When you delete an entry from the keystore file, make sure you leave at least one key pair entry in the keystore file; otherwise, Power Center will not work.

- Scenario 2 — Replace the self-signed certificate with a signed certificate issued by a Certification Authority (CA)

  A certificate signed by a CA is more likely to be trusted by the Web browsers. To sign your certificate by a CA, do the following:

  – Generate a Certificate Signing Request (CSR) and submit to the CA.
  – Import a certificate for your CA.
  – Import the Certificate Reply from the CA.

- Scenario 3 — Import a new Trust Certificate

  Some devices (for example, chassis, or the exposed management interface through WS-MAN) or web service providers may provide a certificate for Power Center validation during the communication establishment. If you validate the certificate, and Power Center fails to verify it by building a trust path from the trust certificate in the keystore file, the communication will fail. In this scenario, you may need to import a new trust certificate to make sure a trust path can be built to verify the certificate.

For more information on how to manage certificates, see Keytool Help.

16

Configuring Power Center

You can configure all the Power Center settings in the **Settings** page. Follow these steps:

1. Click **Edit** on the selected settings.
2. Enter or select a new value.
3. Click **Apply**.

Some settings will take effect immediately; some will not. See the following sections for more specific information.

Monitoring Settings

These settings are used to enable/disable the monitoring and set the sampling interval.

- Monitor all devices and groups — Select to enable or disable monitoring of all devices and groups. The default is **Yes**. If you select **No**, you cannot view the device/group power and temperature details.
- Power sampling interval — Power Center gets power data according to the sampling interval you set (1, 3, or 6 minutes). You can view the power data in the **Power Details** page. The default is 1 minute. For more information on power details, see the "Power Monitoring" chapter.
- Temperature sampling interval — Power Center gets temperature data according to the sampling interval you set (1, 3, or 6 minutes). You can view the temperature data in the **Temperature Details** page. The default is 1 minute. For more information on temperature details, see the "Temperature Monitoring" chapter.

Recommended Sampling Intervals for Performance Tuning and Scaling

It is important to configure appropriate Power and Temperature Sampling Intervals in Power Center. The sampling intervals impact the system performance and footprint significantly, including network bandwidth consumption, database size, and trend graph display latency.

The default power and temperature intervals in Power Center are 1 minute. These value is appropriate for small- or medium-sized environments (where the device number is less than 1000); however, when the environment scales up with more managed devices, you must adjust the values to 3 minutes or 6 minutes.

NOTE: The device number only counts the supported devices. Unsupported devices are not counted.

When are the settings effective?

- Monitor all devices and groups — Immediately.
- Power/Temperature sampling interval — Every 30 minutes in the hour. For example, 08:00, 08:30, 09:00, etc.

Default Units Settings

These settings are used to convert the power/temperature value into your selected units of measurement and display the energy consumption cost in your selected currency.

- Power Units — Select power unit; this unit is used to display the power details. Power Center automatically converts the power values according to the selected unit.
- Temperature Units — Select temperature unit; this unit is used to display the temperature details. Power Center automatically converts the temperature values according to the selected unit.
- Currency — Select currency; this unit is used to display the energy consumption cost. After you change the unit, Power Center does not convert the cost value according to the exchange rate. Power Center only changes the display of the currency symbol.

When are the settings effective?

Immediately.

Protocol Type Device Timeout Settings

These settings are used to configure the timeout between devices and the Power Center server.

- IPMI — Communication timeout between Power Center and an IPMI-enabled device (1-20 seconds). The default is 3 seconds.
- SNMP — Communication timeout between Power Center and a SNMP-enabled device (1-20 seconds). The default is 3 seconds.
- WS-MAN — Communication timeout between Power Center and a WS-MAN device (5-180 seconds). The default is 60 seconds.

When are the settings effective?

From the next time Power Center tries to communicate with the affected device.

Energy Consumption Settings

These settings are used to calculate the energy consumption cost.

- Flat Rate — The rate of the power per kilowatt-hour (kWh); it uses the currency you set in Default Units. The default is 0.
- Cooling Multiplier — The multiplier enables estimating the energy needed to cool the device/group. The default is 1.5. For more information on how the cooling multiplier is applied, see "Viewing Energy Consumption" in the "Power Monitoring" chapter.

When are the settings effective?

- Flat Rate — From beginning of the next hour. For example, if you changed the setting on 8:15, the new setting will be effective from 9:00.
- Cooling Multiplier — Immediately.

SNMP Traps Settings

These settings are used to enable Power Center to send the following custom events to your preferred third-party applications:

- Average Power
- Average Inlet Temperature
- Max Power
- Policy Cannot Be Maintained
- Policy Return To Normal
- Power Return To Normal
- Temperature Return To Normal

For more information on the event details, see "Custom Events" in the "Event Management" chapter.

To send the events to a third-party application, follow these steps:

Step 1. Import the MIB file to your application

1. Find the Power Center MIB file in: <*InstallDir*>\Conf\DellOpenManagePowerCenter-MIB.mib
2. Import the MIB file to your application, see your application Help.

Step 2. Configure the SNMP Trap Settings

1. Click **Edit**.
2. In the **Enabled** field, select **Yes**.
3. Enter the following information:
   - Destination IP/Host — The IP address or host name of the destination device that you want to send events. The maximum length for Destination IP/Host is 255 characters.
   - Port — The port number for the destination device to receive the event traps. You can use any available port between 1-65535.
   - Community Name — A descriptive name of the community, for example: Public. The maximum length for Community Name is 255 characters.
4. Click **Apply**.

NOTE: You can add up to three SNMP Trap receivers.

After you have applied the settings, you can update the settings or run a test for the settings.

To update the settings:

1 Click **Edit**.

2 Enter information for fields Destination IP/Host, Port or Community Name.

NOTE: 1) If the Port field is empty, Power Center will use port 162. After the setting is applied, you can refresh the page to see the port number. 2) If you leave all three fields empty, Power Center will delete this setting. 3) You can leave the Community Name field empty. When it is empty, the SNMP trap message sent by Power Center will not contain a community name.

3 Click **Apply**.

To run a test for the settings:

1 Click **Run Test**.

2 Either a **Success** or **Failed** message appears in this section.

Database Policy Settings

These settings are used to configure the database maintenance policy.

Power Center stores the monitoring data of your data center in the database file. Power center uses compressed power/temperature data to optimize for higher query performance and smallest database size.

Power Center stores both power/temperature compressed data and non-compressed data in the database. Data Compression will aggregate and save the monitoring data using a bigger granularity (hourly or daily), but not the original granularity decided by the Sampling Interval. Data Compression helps to improve the efficiency of data queries.

Power Center keeps compressed power/temperature data and event data up to 365 days and non-compressed power/temperature data up to 14 days.

Configure the length of time that Power Center will keep compressed and non-compressed data using the **Purge Data Older Than** and **Data Compression** fields. The data that exceeds its length of time or is older than the purge date is deleted. This improves the efficiency of the data query. You can automatically purge data by using the **Schedule Database Purging Daily at** field, or you can trigger it manually to start purging data immediately (see the task "To purge the database now").

You can set the following for database maintenance:

- **Data Compression** — You can set the number of the days (1-14) to keep the non-compressed data. The default is 7 days.
- **Purge Data Older Than** — You can set the number of the days (1-365) to keep the compressed data and the event logs. The default is 365 days.
- **Schedule Database Purging Daily at** — You can set the time of day to start database purging (00:00:00 - 23:00:00). The default is 23:00:00.
- **Export Database** — You can export the data in a selected date range to a .csv file. Click **Export Database**, and define a start and end date to export all the data between 00:00:00 of the start date to 00:00:00 of the next day after the end date to a .csv file. By default, the .csv file is saved in the Downloads folder of your Web browser.

  The following data is exported:

  – Measurement data of supported devices (excludes groups) — There is no measurement data for unsupported devices.

  – Hourly data — Hourly data is the data collected during the hour before (timestamp - 1). For example, if the timestamp of the data is 14:00:00, the "PowerAvg" field displays the average power from 13:00:00 to 14:00:00.

  NOTE: If there is no data available at the defined timestamp, this field displays "-1".

  The .csv file includes the following fields:

  – DeviceId — Power Center internal device unique ID.

  – DeviceType — Device type. For example, Server, PDU, UPS and CMC.

  – DeviceName — Device name.

  – DeviceIP — Device IP address.

  – Timestamp — Data timestamp.

  – PowerAvg — Average power value.

  – PowerMin — Minimum power value.

  – PowerMax — Maximum power value.

  – InletTemperatureAvg — Average inlet temperature value.

  – InletTemperatureMin — Minimum inlet temperature value.

– InletTemperatureMax — Maximum inlet temperature value.

After you export data to a .csv file, you can:

– Use Microsoft Excel to open the .csv file and analyze the data, for example, when creating charts using the data.

– Write your own application (or script) to parse the data in the .csv file.

- **Purge Database Now** — You can manually purge the database at anytime. Once you click **Purge Database Now**, Power Center starts to purge the database according to your setting in **Purge Data Older Than** immediately. Once completed, you will see the informative event "Database Maintenance Success" in the **Event Logs** page.

When are the settings effective?

Immediately.

Installation Settings

During Power Center installation, you set the communication settings between the Power Center server and the database, KDC server, and Kerberos pre-authentication. After installation, you can change these settings in the **Settings** page.

- Database settings
- Kerberos Realm settings
- Power Center Server's Domain Account for Kerberos SSO

Database Settings

To change the database connection information, you can configure the database settings in the **Settings** page. Power Center supports database settings changes for local and remote systems.

- Change local database settings: If you install Power Center using local database settings, you can change the settings (except PostgreSQL Host) in the **Settings** page after the installation. Power Center does not support switching from local database to the remote database.
- Change remote database settings: If you install Power Center using the remote database setting, you can change all the settings in the **Settings** page after the installation.

Before changing the database settings, the system must meet the following requirements:

- The correct connection information (Server Name, Database Port, Database User Name, Database User Password) are provided.
- The new database must be an existing Power Center database, and the version of PostgreSQL is 8.3.5.
- If the new database is located on a remote server, the database service on the remote server must be able to accept the remote database connection.

You can configure the following database settings in the **Settings** page:

- PostgreSql Host
- PostgreSql Port
- User Name
- Password

The following sections explain how to change the database settings for local and remote systems. You must start or stop Power Center services when changing the database settings; see your Windows OS service startup/stop method to start or stop all Power Center services.

Change Local Database Settings

To change database settings:

Step 1. Change the database settings in Power Center management console

1. Go to **Settings** → **Database**, and click **Edit**.
2. Enter the following database information:

- PostgreSql Port — PostgreSql port number (default: 6443)
- User Name — PostgreSql database user name
- Password — PostgreSql database user password

NOTE: The new database must have been used by Power Center before.

3. Click **Apply**.
4. Stop all Power Center services on the Power Center server.

Step 2. Change PostgreSQL database settings on the local server

To change the database port, see the following steps:

1. Log into Windows with the Administrator privilege.
2. Open a command line with the Administrator privilege.
3. Run the following command to remove the original database service (The command below assumes Power Center is installed at C:\Program Files\Dell\OpenManagePowerCenter. If Power Center is installed at a different location, substitute the correct location):

   ```
   "C:\Program
   Files\Dell\OpenManagePowerCenter\external\pgsql\bin
   \pg_ctl.exe" unregister -N "Dell OpenManage Power
   Center Database Server"
   ```

4. Run the following commands to create new database services with the new database port (The command below assumes the new database port is 6543. If it is a different port number, substitute the correct number):

   ```
   "C:\Program
   Files\Dell\OpenManagePowerCenter\external\pgsql\bin
   \pg_ctl.exe" register -N "Dell OpenManage Power
   Center Database Server"  -D "C:\Program
   Files\Dell\OpenManagePowerCenter\pgdata"  -o "-F -p
   6543"
   ```

5. Run the Dell OpenManage Power Center Database Server service using the Network Service account. For more information on how to run the service using a Network Service account, see Windows Help. The following is an example for Windows 7:
   a. Open **Computer Management** → **Services and Applications** → **Services**, and then select the **Dell OpenManage Power Center Database Server** service, right-click and select **Properties**.
   b. In the **Properties** window, click the **Log On** tab. Go to **This Account** field, enter the Network Service account information, then click **OK**.
6. Start the **Dell OpenManage Power Center Database Server** service. If you can start this service, all the settings in previous steps are correct.

To change the database user name or password, perform the following steps:

1. Log into Windows with the Administrator privilege.
2. Stop the **Dell OpenManage Power Center Database** Server service.

3 Change the pg_hba.conf file (By default, pgdata of Power Center is installed at C:\Program Files\Dell\OpenManagePowerCenter\pgdata):

Original:

```
# IPv4 local connections:

host    all         all         127.0.0.1/32
password
```

New:

```
# IPv4 local connections:

host    all         all         127.0.0.1/32
trust
```

4 Start **Dell OpenManage Power Center Database Server** service.

5 To change the user name, run the following commands (The command below assumes Power Center is installed at C:\Program Files\Dell\OpenManagePowerCenter and NewName is the new user name):

```
"C:\Program
Files\Dell\OpenManagePowerCenter\external\pgsql\bin
\psql.exe" -p 6443 -U postgres -d dcmapp -c "ALTER
ROLE dcmdba RENAME TO NewName;"
```

NOTE: If you change the user name, you must reset the password.

6 To change the password, run the following commands (The command below assumes Power Center is installed at C:\Program Files\Dell\OpenManagePowerCenter NewPassword is the new password):

```
"C:\Program
Files\Dell\OpenManagePowerCenter\external\pgsql\bin
\psql.exe" -p 6443 -U postgres -d dcmapp -c " ALTER
Role dcmdba PASSWORD 'NewPassword';"
```

7 Stop the **Dell OpenManage Power Center Database Server** service.

8 Restore "C:\Program Files\Dell\OpenManagePowerCenter\pgdata\pg_hba.conf file" to the original value, see the following commands (By default, pgdata of Power Center is installed at C:\Program Files\Dell\OpenManagePowerCenter\pgdata):

Current value:

```
# IPv4 local connections:

host    all         all         127.0.0.1/32
trust
```

Replace to original value:

```
# IPv4 local connections:

host    all         all         127.0.0.1/32
password
```

9 If you can log in with the new user name or password using the pgAdmin tool, all the settings in the previous steps are correct.

Step 3. Start all Power Center services

Start all Power Center services.

Change Remote Database Settings

Power Center supports switching from a remote database to the other remote database; however, the other remote database must have already been used by Power Center before switching to it.

Step 1. Change database settings in the Power Center management console

1 Go to **Settings** → **Database**, and click **Edit**.

2 Enter the following database information:

- PostgreSql Host — Host name or IP address (default: localhost)
- PostgreSql Port — PostgreSql port number(default: 6443)
- User Name — PostgreSql database user name
- Password — PostgreSql database user password

3 Click **Apply**.

4 Stop all Power Center services on the Power Center server.

Step 2. Enable remote database to accept a remote connection

By default, the Power Center database only accepts local host connection requests. If you change the Power Center database to remote Power Center database (on another server), the Power Center service will not start. Use the following example for stopping and restarting the Power Center services:

The following steps assume local host is 192.168.11.11, remote database host is 192.168.11.22, and the remote database folder is located at C:\Program Files\Dell\OpenManagePowerCenter\pgdata.

On the remote database host:

1. Stop the **Dell OpenManage Power Center Database Server** service.
2. Add your OS user with Read/Write permission to "C:\Program Files\Dell\OpenManagePowerCenter\pgdata\postgresql.conf" and "C:\Program Files\Dell\OpenManagePowerCenter\pgdata\pg_hba.conf".

   Refer to your operating system documentation for instructions on how to change file privileges.
3. Open "C:\Program Files\Dell\OpenManagePowerCenter\pgdata\postgresql.conf" with a text editor and update the following:

- Original value — `"listen_addresses = 'localhost'"` , this means that the database services will only serve connection requests from a local host.
- New value — `"listen_addresses = '*'"` , this means that the database services will serve connection requests from all hosts.

4. Open "C:\Program Files\Dell\OpenManagePowerCenter\pgdata\pg_hba.conf" with a text editor and add the following:

- Original value (Only accepts local host connection requests) —

  ```
  # IPv4 local connections: host all all 127.0.0.1/32 password
  ```

- New value (Accepts connection requests from local host and (192.168.11.11) —

  # IPv4 local connections:

  ```
  host all all 192.168.11.11/32 password
  ```

  ```
  host all all 127.0.0.1/32 password
  ```

5. Start the **Dell OpenManage Power Center Database Server** service.

NOTE: For more information on PostgreSQL client authentication, see **http://www.postgresql.org/docs/8.3/static/client-authentication.html**.

Step 3. Change PostgreSQL database settings on a remote server

See "Change database settings in PostgreSQL database" in the "Change to Database on the Local Systems" section of this chapter.

Step 4. Start all Power Center services

Start all Power Center services.

Kerberos Realm Settings

You can configure the following Kerberos realm settings in the **Settings** page:

- Realm Name — Domain Name of KDC server
- KDC Server — Address of KDC server; either IP address or server name

You must restart Power Center services after you make the changes.

When are the settings effective?

After restarting all Power Center services.

For more information on how to restart Power Center services, see "Power Center Services" in the "Installing and Launching" chapter.

Power Center Server's Domain Account for Kerberos SSO

You can configure the following Kerberos SSO pre-authentication settings in the **Settings** page:

- User Name — User name for Kerberos pre-authentication account
- Password — Password for Kerberos pre-authentication account

When are the settings effective?

Immediately.

For more information on Kerberos pre-authentication settings, see "Installing Power Center" in the "Installing and Launching" chapter.

17

Backup and Recovery

You can back up and recover the data in Power Center.

To support Power Center recovery, you must back up Power Center data first. Power Center only supports complete backup and recovery. It does not support incremental backup and recovery.

NOTE: You should back up Power Center data on a regular basis.

You may need to start or stop Power Center services during the backup and recovery. For more information on Power Center services, see "Power Center Services" in the "Installing and Launching" chapter. For more information on how to start or stop Power Center services, see your Windows Help.

Power Center Data

Power Center data is defined as the following three categories:

Table 17-1. Power Center Data

Category	Files	Description
Configuration files	app.config.xml	
	user.config.xml	
	web.config.xml	
	server.xml	
	login.conf	
	krb5.conf	
	java.security	
Key store file	keystore.ssl	
Database data file	pgdata	This is a folder. Power Center utilizes PostgreSQL to store data. Pgdata is a standard PostgreSQL data folder.

For a Power Center installation in C:\Program Files\Dell\OpenManagePowerCenter, the data files are located as follows:

C:\Program Files\Dell\OpenManagePowerCenter\conf\app.config.xml

C:\Program Files\Dell\OpenManagePowerCenter\conf\user.config.xml

C:\Program Files\Dell\OpenManagePowerCenter\conf\web.config.xml

C:\Program Files\Dell\OpenManagePowerCenter\external\apache-tomcat\conf\server.xml

C:\Program Files\Dell\OpenManagePowerCenter\external\jre\lib\security\login.conf

C:\Program Files\Dell\OpenManagePowerCenter\external\jre\lib\security\krb5.conf

C:\Program Files\Dell\OpenManagePowerCenter\external\jre\lib\security\java.security

C:\Program Files\Dell\OpenManagePowerCenter\keystore.ssl

C:\Program Files\Dell\OpenManagePowerCenter\pgdata

Power Center Backup

When you back up Power Center, follow the steps below:

1. Stop all Power Center services.
2. Back up all Power Center data.
   a. Refer to your operating system documentation for instructions on how to change file privileges; you need to add your OS user with the Read privilege for the files listed in the Power Center Data table. You must add the Read privileges to all sub-contents of the pgdata folder.
   b. Local: Copy all these Power Center data files to your backup location. Remote: Copy all these Power Center data files to your backup location except the pgdata folder. You must back up the database (i.e., pgdata) on the remote server following the PostgreSQL backup and recovery Web pages.

NOTE: For the PostgreSQL database file pgdata, if you want to do customized database backup/recovery, such as incremental backup/recovery, see the PosetgreSQL backup and recovery Web page at: **http://www.postgresql.org/docs/8.3/interactive/backup.html**.

3 Start all Power Center services.

The Power Center backup is completed.

Power Center Recovery

When you recover Power Center data, follow the steps below for a complete recovery:

1 Install Power Center with the same version and same user inputs as the original installation.

2 Stop all Power Center services.

3 Recover all Power Center data files.

a Refer to your operating system documentation for instructions on how to change file privileges; you need to add your OS user with the Read and Write privileges for the files listed in the Power Center Data table.

NOTE: Record your actions, because these privileges will be removed later.

b **Local:** Replace all of the Power Center data files above with your backup files except server.xml and java.security. **Remote:** Replace all of the Power Center data files above with your backup files except server.xml and java.security and pgdata folder. Follow the PostgreSQL backup and recovery Web page to recover the remote database. (For both local and remote: for best results, rename these files for backup, and copy backup files to this location).

c For server.xml, you must manually update its parameters with the parameters in the original server.xml backup file.

1) Update SSL port:

Replace the following highlighted value with the value in the server.xml backup file.

```
<Connector port="8688" protocol="HTTP/1.1"
server="localhost" maxHttpHeaderSize="8192"

connectionTimeout="60000" xpoweredBy="false"
allowTrace="false" scheme="http" redirectPort=
"8643"/>

<Connector protocol=
"org.apache.coyote.http11.Http11Protocol"  port=
```

```
"8643" minSpareThreads="5" maxSpareThreads="75"
maxHttpHeaderSize="8192"  enableLookups="true"
disableUploadTimeout="true" connectionTimeout=
"60000" acceptCount="100" maxThreads="200"
server="localhost" allowTrace="false" scheme=
"https" secure="true" SSLEnabled="true"
xpoweredBy="false" keystoreFile="E:\Program

Files\Dell\OpenManagePowerCenter\keystore.ssl"
keystorePass="DCM10!pass"  clientAuth="false"
sslProtocol="TLS"/>
```

2) Update the Keystore path:

Replace value below in bold with the actual location of recovered keystore.ssl file.

```
<Connector protocol=
"org.apache.coyote.http11.Http11Protocol"  port=
"8643" minSpareThreads="5"

maxSpareThreads="75" maxHttpHeaderSize="8192"
enableLookups="true" disableUploadTimeout="true"
connectionTimeout="60000" acceptCount="100"
maxThreads="200" server="localhost" allowTrace=
"false" scheme="https" secure="true" SSLEnabled=
"true" xpoweredBy="false" keystoreFile=
"E:\Program
Files\Dell\OpenManagePowerCenter\keystore.ssl"
keystorePass="DCM10!pass"  clientAuth="false"
sslProtocol="TLS"/>
```

3) Update the Keystore password:

Replace the value below in bold with the value in the server.xml backup file.

```
<Connector protocol=
"org.apache.coyote.http11.Http11Protocol"  port=
"8643" minSpareThreads="5"

maxSpareThreads="75" maxHttpHeaderSize="8192"
enableLookups="true" disableUploadTimeout="true"
```

```
connectionTimeout="60000" acceptCount="100"
maxThreads="200" server="localhost" allowTrace=
"false"

scheme="https" secure="true" SSLEnabled="true"
xpoweredBy="false" keystoreFile="E:\Program

Files\Dell\OpenManagePowerCenter\keystore.ssl"
keystorePass="DCM10!pass"  clientAuth="false"
sslProtocol="TLS"/>
```

d For java.security, you must manually update the l*ogin.config.url.1* parameter with value *file*:${*java.home*}/*lib/security/login.conf*. For example:

login.config.url.1=file:${*java.home*}/*lib/security/login.conf*

e Refer to your operating system documentation for instructions on how to remove file privileges, you need to remove the privileges that you have added for the files.

NOTE: Make sure the account that Power Center services is logged on with the Full Control privilege to the Power Center data files (see "Power Center Data" section in this chapter). Otherwise, the recovery may fail. For example, if Power Center services are logged on with the Network Service (default) account, and this account has no Full Control privilege to the recovered pgdata folder, the Dell OpenManage Power Center Database Server service will not start and the recovery will fail.

4 Start all Power Center services.

The Power Center recovery is completed.

NOTE: When you change the Read/Write privileges for the files listed in the Power Center Data table, to make sure the success of backup or recovery, double-check the privileges before proceeding to the next step.

18

Troubleshooting

This chapter lists some of the known issues you may encounter when working with Power Center, and some possible solutions.

- **Problem1:** Not able to access the Power Center management console from the client browser, even though the Power Center server is running normally.
  - **Cause:** The proxy setting may prevent the browser from accessing the Power Center server on the network.
  - **Resolution:** Check your proxy setting and make sure it is properly configured.
- **Problem 2:** Cannot play video when clicking the video links in the **Getting Started** page.
  - **Cause:** You do not have a flash player installed for your Web browser.
  - **Resolution:** Install the latest version of Adobe Flash Player for your Web browser.
- **Problem 3** You have been logged out of Power Center automatically.
  - **Cause:** Possible causes include: 1) The network connection is lost. 2) Your user account has been deleted.
  - **Resolution:** 1) Check your network connection status; make sure it is connected to the Power Center server. 2) Check your user account status; make sure it is not deleted by another user with higher privileges.
- **Problem 4:** The network connection status is connected, but you failed to connect to Dell iDRAC6 devices (Dell PowerEdge Servers).
  - **Cause:** Dell iDRAC6 devices are limited to three concurrent connection sessions; you have reached the limitation of connection sessions. There are various reasons that may cause the session to be occupied for a while until it is relinquished, for example, you used incorrect credential information to connect with Dell iDRAC6 devices for three times or more within a short period.

- **Resolution:** Wait one minute or more for Dell iDRAC6 devices to release the connection sessions, then try again.

- **Problem 5:** Power Center cannot receive events sent from devices.
  - **Cause:** Possible causes include: 1) Power Center is not the destination host of the events sent from devices. 2) There is a network connection problem. 3) The essential services are not started.
  - **Resolution:** Make sure that: 1) The Power Center server's IP address is registered on the device as the destination for the events. 2) The network of the device and the Power Center server is connected and packets can be routed to each other. 3) If the Windows SNMP Trap service is installed on the Power Center server, this service and the Dell OpenManage Power Center SNMP Dispatcher shall be started on the Power Center server.
- **Problem 6:** If Power Center uses a remote database during the installation, the error message "server side error has occurred, please contact support" displays when you launch the Power Center management console.
  - **Cause:** The connection between Power Center and the remote database server is lost because the IP or hostname of the remote database server has been changed.
  - **Resolution:** 1) Change the IP or hostname of the remote database to the previous value. 2) Update the Power Center configuration files with the new database server address. Perform the following steps (These steps assume that Power Center is installed at C:\Program\Files. If Power Center is installed at a different location, substitute the correct location.): a) Assign the current OS user with Read and Write privileges to the configuration files "app.config.xml" and "user.config.xml" located at C:\Program Files\Dell\OpenManagePowerCenter\conf\. b) Open the two files with a text editor. c) Change the DB_SERVER_NAME value to a new database server IP or hostname. d) Remove the privileges that you assigned to the configuration files in Step a. e) Restart all the Power Center services and launch the Power Center management console again.
- **Problem 7:** The Firefox Web browser crashes when it has been running for a long time.

- **Cause:** Firefox may have a memory leak after running for a long time. The memory leak-related issues may cause Firefox to function improperly.
- **Resolution:** Restart the Firefox Web browser and log into Power Center again.

- **Problem 8:** Cannot see the Power/Temperature data in the **Dashboard** tab.
  - **Cause:** You may have changed the settings of the Power/Temperature sampling intervals. Before the new settings take effect, the Power/Temperature data may be temporarily unavailable.
  - **Resolution:** Wait until the new settings take effect. For more information on when the settings are effective, see "Monitoring Settings" in the "Configuring" chapter.
- **Problem 9:** Power Center is corrupted or uninstalled, but the previously-existing power policies (including EPR) on the devices are still effective.
  - **Cause:** Even if Power Center is corrupted or uninstalled, the Power Cap Values of the existing power policies (including EPR) on the devices still remain effective.
  - **Resolution:** Check your data center power capacity to avoid tripping the breaker before performing the following steps. 1) If you uninstall Power Center, make sure you have removed all devices before uninstalling. 2) If Power Center is corrupted, do one of the following to remove the power policies: 2.1) If the device number is small, access the Dell iDRAC management console, and manually remove the power policies. 2.2) If the device number is large, perform the following steps: a) Install Power Center. b) Add all the devices to the Power Center management console. c) Create a logical group that contains all these devices, then create any power policy for this group. d) Remove all these devices from the Power Center management console. After completing the steps a-d, Power Center will remove the policies first, then remove the devices.
- **Problem 10:** A PostgreSQL error log "FATAL: terminating connection due to administrator command" occurred in the Windows event log.
  - **Cause:** This is caused by Power Center server shutdown. Normally the Power Center database service (Dell OpenManage Power Center Database Server service) will stop after other Power Center services, but if the Power Center server has been shut down quickly, the Power

Center database service will be forced to stop when other Power Center services are not yet stopped yet. In this case, the database connection sessions that cannot be closed by other Power Center services will be closed by the Power Center database service, and this error is generated. Since such an error is caused by Windows when it shuts down the services quickly, Power Center will protect its important data through transaction; therefore, this kind of error does not impact Power Center.

– **Resolution:** No action is required.